UNIVERZITA KARLOVA V PRAZE
PRÁVNICKÁ FAKULTA
Katedra pracovního práva a práva sociálního zabezpečení

RIGORÓZNÍ PRÁCE

Ochrana osobních údajů v pracovněprávních vztazích

Personal Data Protection in Labour Law Relationships

Konzultant: doc. JUDr. Jan Pichrt, Ph.D.

Zpracovatel: Mgr. Alice Mlýnková

ÚNOR 2012

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že jsem předkládanou rigorózní práci vypracovala samostatně za použití zdrojů v ní uvedených. Všechny použité prameny a literatura byly řádně citovány a práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne __. __. 2012 ……

Mgr. Alice Mlýnková

PODĚKOVÁNÍ

Děkuji velice svému manželovi za veškerou podporu a trpělivost, kterou mi poskytoval a poskytuje nejen během přípravy této práce.

Rovněž bych ráda poděkovala svému konzultantovi doc. JUDr. Janu Pichrtovi, Ph.D. za cenné připomínky a rady, zejména pokud se týká směřování celé práce.

Zkratky

antidiskriminační zákon	Zákon č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací, ve znění pozdějších předpisů
Listina základních práv a svobod	Usnesení č. 2/1993 Sb. Předsednictva České národní rady o vyhlášení Listiny základních práva a svobod jako součásti ústavního pořádku České republiky
NS	Nejvyšší soud
občanský zákoník, ObčZ	Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů
Směrnice	Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24.10.1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
Úmluva 108	Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (č. 108)
Úřad, ÚOOÚ	Úřad pro ochranu osobních údajů
WP 29, Pracovní skupina 29	Pracovní skupina (Working Party) zřízená na základě čl. 29 směrnice č. 95/46/ES; nezávislý evropský poradní orgán v oblasti ochrany údajů a soukromí
Zákon, ZOOÚ	Zákon č. 101/2000 Sb. o ochraně osobních údajů, ve znění pozdějších předpisů
zákoník práce, ZP	Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
zákon o zaměstnanosti, ZZ	Zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů

Úvod

Osobní údaje a jejich ochrana se staly fenoménem současné doby, ve které „kdo není na síti, jako by nebyl“. S rozšířením vysokorychlostního internetu do převážné většiny domácností se za poslední desetiletí udála jakási malá datová revoluce. Informace, které dříve měly soukromou povahu a zůstávaly vyhrazeny nejbližším přátelům, dnes jediným kliknutím dáváme na odiv celému světu, aniž bychom si uvědomovali, kdo všechno může být na druhé straně „drátu“. Velice často však ani nemáme na vybranou: ekonomické subjekty jako by za hodnotnější klienty a zákazníky považovaly ty, kdo si založí klubovou nebo věrnostní kartu, zúčastní se spotřebitelské soutěže či internetového hlasování – a to vše samozřejmě za současného poskytnutí osobních údajů. V některých případech dokonce se zpracováním svých osobních údajů nejsou dotčené osoby ani seznámeny, byť jsou tyto případy stále vzácnější.

Není proto divu, že s rostoucími možnostmi sdílení a zpracování osobních údajů narůstá také zájem jednotlivců na jejich ochraně. V současnosti, kdy moderní technologie umožňují velmi snadné získávání a předávání informací, může jednotlivec velice snadno ztratit přehled o tom, komu či kam byly jeho osobní údaje předány a kde všude mohou být uloženy pro pozdější využití. Ač povědomí o důležitosti ochrany osobních údajů jedince a tím i ochrany jeho soukromí zřetelně stoupá, zůstává stále postoj nemalé části populace k nakládání s vlastními osobními údaji poměrně lehkomyslný, což neoprávněné zpracování osobních údajů do značné míry usnadňuje. I proto při kontrole nakládání s osobními údaji fyzických osob hrají nezanedbatelnou roli orgány státní správy v čele s Úřadem pro ochranu osobních údajů.

Osobní údaje konkrétních subjektů přitom představují nesmírně cenný zdroj informací – čím rozsáhlejší je jejich znalost, tím více je možné z těchto informací ve vztahu ke konkrétní osobě vytěžit, a to především ekonomicky. Způsoby shromažďování a zpracovávání již získaných osobních údajů se tak s vidinou snazšího dosažení zisku stávají stále propracovanějšími, což snižuje

pravděpodobnost, že budou případy neoprávněného zpracování údajů ze strany příslušných orgánů odhaleny. Výpočetní technika navíc v současnosti umožňuje soustředit v podstatě neomezené množství osobních údajů na minimální ploše; s údaji lze přitom manipulovat jak jednotlivě, tak hromadně, vzájemně je kombinovat, jejich jednotlivé součásti spojovat s jinými, a tak stále více odkrývat integritu nejen subjektu údajů, ale i jeho okolí[1].

Nabízí se však otázka, z jakého důvodu a zda by ochrana osobních údajů měla být regulována právními předpisy a nemělo-li být ponecháno na uvážení každého jednotlivce, zda a komu své osobní údaje sdělí a jakým způsobem bude dbát o jejich ochranu. V běžném životě však většina jednotlivců nemá na výběr, a pokud chtějí vstupovat do nejrůznějších smluvních vztahů, osobní údaje třetím osobám jednoduše poskytovat musí. Škála smluvních partnerů je v těchto případech velice široká - od zaměstnavatele přes telefonního operátora až po provozovatele mateřské školky. Jelikož velká část těchto smluvních vztahů je uzavírána mezi jednotlivcem a právnickými osobami, které subjektem osobních údajů být nemohou, ocitá se fyzická osoba jako nositel osobních údajů vůči těmto korporacím v nerovném postavení.

Cílem regulace v oblasti ochrany osobních údajů proto není zabránit zpracování osobních údajů, neboť to v současnosti není dost dobře možné a s ohledem na další rozvoj společnosti ani žádoucí, nýbrž jejím cílem je zajistit adekvátní ochranu údajů fyzických osob při zpracování další osobou takovým způsobem, aby nedošlo k jejich zneužití a neoprávněnému zásahu do soukromí fyzických osob, případně aby k takovému zásahu došlo pouze v nezbytné míře a přiměřeném rozsahu.

Stejně jako v ostatních smluvních vztazích, tedy i v pracovněprávních vztazích tak nevyhnutelně dochází ke zpracování osobních údajů. Zpracování určitých osobních údajů zaměstnanců je dokonce vyžadováno pracovněprávními předpisy, dle kterých musí zaměstnavatel před vznikem, v průběhu a dokonce i po

[1] Mates, P. *Ochrana osobních údajů.* 1. vyd. Praha: Karolinum, 2002, s. 39.

zániku pracovněprávního vztahu disponovat relativně velkým rozsahem informací o zaměstnanci, a chce-li dostát svým zákonným povinnostem vůči orgánům státní správy a dalším subjektům, nemůže zcela dle vlastního uvážení rozhodovat, zda tyto osobní údaje zaměstnanců bude či nebude zpracovávat.

Zaměstnavatelé však často shromažďují osobní údaje zaměstnanců či uchazečů od zaměstnání i ve větším rozsahu než požaduje zákon, neboť se domnívají se, že širší znalost údajů týkajících se zaměstnance jim umožní zefektivnit produktivitu jeho práce a zvýšit jeho motivaci na pracovních výsledcích, které jsou nedílnou součástí podnikatelského úspěchu zaměstnavatele. Zaměstnanec je tedy nucen poskytovat své osobní údaje cizí osobě (byť v podobě zaměstnavatele), na které je finančně závislý a vůči které je v podřízeném vztahu. V případě poskytování údajů zaměstnanců v rámci koncernových uskupení navíc zaměstnanci často ani netuší, komu své osobní údaje vlastně poskytují, neboť jejich údaje bývají předávány ke zpracování centrálám v zahraničí, které k jejich zpracování mohou využít i další osoby. Proto je na správních orgánech a zejména Úřadu pro ochranu osobních údajů, aby efektivně vedly nejen zaměstnavatele, nýbrž všechny osoby zpracovávající osobní údaje k dodržování právních předpisů na tomto poli. Pouze tak je možné dosáhnout dostatečné míry ochrany osobních údajů fyzických osob, potažmo práva na ochranu soukromí člověka jako jednoho ze základních lidských práv člověka.

Cílem této práce by proto mělo být přispět k pochopení podstaty ochrany osobních údajů v pracovněprávních vztazích s ohledem na rozsáhlé možnosti využití vyspělých technologií, a to jak z pohledu zaměstnavatele, tak z pohledu zaměstnance. Zaměstnavatelé při své činnosti často naráží na otázky z této oblasti, na něž však zatím právní předpisy jednoznačné odpovědi neposkytují. I proto považuji za důležité se některými z těchto otázek zabývat a snažit se nalézt řešení, která by na jedné straně umožňovala zaměstnavatelům plně využívat potenciál svých zaměstnanců, avšak na druhé straně respektovala ústavně zaručené právo zaměstnance na ochranu soukromí. Mým záměrem není rozebírat detailně definice či jednotlivá práva a povinnosti související se zpracováním osobních údajů; ráda

bych se však více zabývala praktickou stránkou věci, a to především v části zabývající se vybranými problematikami v pracovněprávních vztazích. Problematika ochrany osobních údajů jednotlivce rozhodně není uzavřenou kapitolou, v níž by byly všechny otázky zodpovězeny a všechna pravidla jasně stanovená. S nutností reakce na nové technologie umožňující další a hlubší způsoby zásahu do soukromí jednotlivců se stále znovu otevírá prostor pro řešení dosud nevyjasněných otázek při hledání rovnováhy mezi právem na ochranu soukromého života fyzických osob a ochraně odůvodněných zájmů správců jejich osobních údajů.

1. Právní úprava ochrany osobních údajů

Ochrana osobních údajů, a to samozřejmě nejen v pracovněprávních vztazích, primárně souvisí s ochranou soukromí člověka, tedy jeho osobní sféry a integrity zahrnující všechny jeho projevy[2]. Teprve však po skončení druhé světové války, s postupným rozvojem chápání a rozšiřování rozsahu lidských práv a základních svobod (tzv. lidská práva druhé a především třetí generace), došlo k zakotvení práva na ochranu soukromí jednotlivce a rodinného života ve významných lidsko-právních mezinárodních dokumentech jako jsou Všeobecná deklarace lidských práv z roku 1948 (čl. 12), Evropská úmluva o ochraně lidských práv a základních svobod z roku 1950 (čl. 8) či Mezinárodní pakt o občanských a politických právech z roku 1966 (čl. 17). Otázka pojetí soukromí člověka se také stala předmětem mnoha soudních rozhodnutí, a to zejména Evropského soudu pro lidská práva, zřízeného k projednávání porušení Evropské úmluvy o ochraně lidských práv a základních svobod. Na některá z těchto rozhodnutí odkazuje také nález Ústavního soudu sp.zn. II.ÚS 517/99, v němž Ústavní soud odmítl zúžené pojetí práva na ochranu soukromí fyzické osoby a zdůraznil, že „respektování soukromého života musí zahrnovat do určité míry i právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi“. Postupem času se tak právo na soukromí stalo jedním z nejrozsáhlejších tzv. osobnostních práv[3], neboť při zásahu do soukromí neoddělitelně dochází i k zásahu do všech ostatních osobnostních práv[4].

Jako samostatná část práva na ochranu soukromí se ochrana osobních údajů fyzických osob poprvé závazně vydělila v Úmluvě o ochraně osob se zřetelem na automatické zpracování osobních dat („Úmluva 108“), kterou Rada Evropy otevřela k podpisu v roce 1981. Vytvoření Úmluvy 108 bylo výsledkem několikaleté snahy o reakci na překotný rozvoj technologií v 50. a 60. letech

[2] Stanovisko ÚOOÚ č. 6/2009 – Ochrana soukromí při zpracování osobních údajů.
[3] Jako je kromě dalších i právo na zachování lidské důstojnosti, osobní cti a ochranu vlastního jména, jakož i projevů osobní povahy, včetně již výše uvedeného práva na ochranu soukromí a rodinného života.
[4] Mates, P. *Ochrana osobních údajů.* 1. vyd. Praha: Karolinum, 2002, s. 37.

minulého století, v důsledku čehož se tehdejší právní úprava oblasti ochrany osobních údajů rychle stávala zastaralou a nedostačující[5]. Zkušenosti navíc postupně ukázaly, že ochranu osobních údajů není možné s ohledem na rostoucí objem přenášených údajů mezi státy, jakož i zvyšující se pohyb lidí bez ohledu na hranice jednotlivých států, řešit výlučně na národní úrovni[6]. Česká republika podepsala Úmluvu 108 dne 8. září 2000 a proces její ratifikace byl ukončen 9. července 2001, přičemž k její publikaci došlo ve Sbírce mezinárodních smluv pod č. 115/2001. Jak Úmluva 108 uvádí ve svém prvním článku, jejím účelem je zaručit každé fyzické osobě na území každé smluvní strany úctu k jejímu právu na soukromý život, se zřetelem k automatizovanému zpracování osobních údajů, které se k ní vztahují. V Hlavě II. pak Úmluva obsahuje výčet základních zásad ochrany osobních údajů, které se smluvní strany zavazují na svém území prostřednictvím národních právních řádů zaručit (poctivé získání osobních údajů, jejich oprávněné a účelu přiměřené zpracování, adekvátní zabezpečení, dodatečné záruky subjektu a stanovení prostředků pro postihování porušení těchto pravidel). Úmluva byla dále v r. 2001 rozšířena Dodatkovým protokolem o orgánech dozoru a toku dat přes hranice, k němuž Česká republika přistoupila v r. 2002[7]. Ochraně osobních údajů se také věnuje řada dalších dokumentů Rady Evropy[8].

V českém právním řádu vychází úprava ochrana soukromí jednotlivce ze zákona č. 2/1993 Sb., tzv. Listiny základních práv a svobod (dále jen „Listina základních práv a svobod“), která je součástí ústavního pořádku České republiky. Ta ve svém článku 10 odst. 2, mezi ostatními lidskými právy a svobodami, stanovuje právo každého na ochranu před neoprávněným zasahováním do soukromého a rodinného života, nedotknutelnost osoby a jejího soukromí pak zaručuje článek 7. S právem na ochranu soukromí také úzce souvisí právo na

[5] „Důvodová“ zpráva k Úmluvě 108, dostupná z http://conventions.coe.int/treaty/en/Reports/Html/108.htm.
[6] Bartík, V. Janečková, E. *Zákon o ochraně osobních údajů s komentářem.* 1. vyd. Olomouc: ANAG, 2010, s. 10.
[7] Publikováno pod č. 29/2005 Sb.m.s.
[8] Například Doporučení č. R (89) 2 o ochraně osobních údajů používaných pro účely zaměstnání, Doporučení č. R (86) 1 o ochraně osobních údajů používaných pro účely sociálního zabezpečení nebo Doporučení č. R (99) 5 týkající se ochrany soukromí na internetu.

uchování tajemství o obsahu doručovaných zpráv zaručeným v článku 13 Listiny základních práv a svobod, které zaručuje zachování listovního tajemství i tajemství jiných písemností a záznamů, ať už uchovávaných v soukromí nebo zasílaných poštou či jiným způsobem, a rovněž i tajemství zpráv podávaných telefonem nebo podobným zařízením, a také právo na nedotknutelnost obydlí zaručené v článku 12. V článku 10 odst. 3 Listiny základních práv a svobod je dále zakotveno právo každého člověka na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě, k jehož provedení slouží zvláštní zákon o ochraně osobních údajů[9]. Ochranu před neoprávněnými, avšak jednorázovými zásahy do soukromí jednotlivce pak poskytuje ustanovení § 11 a následující zákona č. 40/1964 Sb., občanský zákoník (dále jen „občanský zákoník" nebo „ObčZ"), v rámci ochrany osobnosti.

Jedním z prvních českých právních předpisů týkající se přímo ochrany osobních údajů byl zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, který však trpěl mnohými nedostatky včetně omezené věcné působnosti (zákon se vztahoval zejména na ochranu informací při provozování informačního systému) a jeho realizace v praxi byla značně obtížná. K odstranění nedostatečného zakotvení ochrany osobních údajů v českém právním řádu tak do značné míry přispěla až snaha o přistoupení k Evropské unii a s tím související povinnost harmonizace národních předpisů s právem Evropské unie (resp. Evropských společenství). Směrnice Evropského parlamentu a Rady č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem těchto údajů („Směrnice") sice primárně vychází z Úmluvy 108, významně ji však rozšiřuje a prohlubuje[10]. Cílem Směrnice je jednak zajistit právo na ochranu soukromí v jednotlivých členských státech, jednak ovšem při jeho dodržení také umožnit volný pohyb osobních údajů z jednoho členského státu do druhého a tím zlepšit fungování vnitřního trhu, přičemž obojího mělo být dosaženo zejména sblížením jednotlivých národních právních řadů, a to v oblasti jak

[9] Srov. dokument sub. pozn. č. 2.
[10] Srov. dokument sub. pozn. č. 6 , s. 11.

automatizovaného, tak manuálního zpracování osobních údajů fyzických osob[11]. Na ochranu osobních údajů právnických osob, stejně jako na zvukové, obrazové a anonymizované osobní údaje se Směrnice nevztahuje. Na překotný technologický rozvoj a nové problematiky na poli ochrany osobních údajů v návaznosti na Směrnici reagovaly i další směrnice týkající se např. elektronického obchodu[12] či elektronických komunikací, jakož i rozhodnutí Komise v souvislosti s předáváním osobních údajů do třetích zemí.

V souvislosti s výše uvedenými předpisy ES/EU byl v dubnu roku 2000 přijat zákon č. 101/2000 Sb., o ochraně osobních údajů („ZOOÚ“ nebo „Zákon“) jako stěžejní zákonná úprava nakládání s osobními údaji, na nějž navazují speciální ustanovení obsažená v jiných právních předpisech. Na rozdíl od právní úpravy v občanském zákoníku poskytuje ochranu před neoprávněnými zásahy do soukromí člověka, k nimž dochází systematickým (tj. nikoliv pouze nahodilým) zpracováním projevů osobní povahy či dalších informací týkajících se konkrétní osoby (jejích osobních údajů) a stanoví pravidla pro jejich zpracování. Zákon o ochraně osobních údajů tak de facto zásahy do soukromí jednotlivce připouští, ovšem pouze za stanovených podmínek, tj. zejména způsobem a prostředky, které Zákon připouští, v přiměřeném rozsahu a za legitimním, dopředu stanoveným účelem. Před zpracováním osobních údajů, které tyto podmínky nesplňuje, a ohrožuje tak soukromí člověka, poskytuje Zákon prostředky k jeho ochraně[13].

Zákon se vztahuje na osobní údaje, které zpracovávají všechny fyzické a právnické osoby, jakož i orgány veřejné moci, a to bez ohledu na to, jakými prostředky ke zpracování dochází. Nevztahuje se na zpracování osobních údajů, které provádí fyzická (nikoli však právnická) osoba výlučně pro osobní potřebu, a ani na jejich nahodilé shromažďování, nejsou-li pak tyto údaje dále zpracovávány. Územní působnost Zákona se vztahuje i na zpracování osobních údajů subjekty,

[11] Srov. např. Sdělení Komise ze dne 4.11.2000 – Komplexní přístup k ochraně osobních údajů v Evropské unii, dostupné z http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_cs.pdf

[12] Směrnice Evropského parlamentu a Rady č. 2000/31/ES ze dne 8.6.2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu

které nemají sídlo na území České republiky, a to zejména tehdy, provádí-li na území České republiky zpracování subjekt usazený mimo Evropskou unii, a to prostřednictvím subjektu nacházejícím se v České republice (např. organizační složka zahraniční společnosti)[14]. Na základě Zákona také v roce 2001 došlo ke zřízení Úřadu pro ochranu osobních údajů („Úřad" nebo „ÚOOÚ") se sídlem v Praze jako ústředního správního úřadu pro oblast ochrany osobních údajů[15]. Jak Úřad uvádí na svých webových stránkách[16], jeho hlavními úkoly jsou dozor nad dodržováním Zákonem stanovených povinností při zpracování osobních údajů, vedení registru povolených zpracování osobních údajů, přijímání podnětů a stížnosti ze strany občanů, jakož i poskytování konzultací v oblasti ochrany osobních údajů.

Zákon na ochranu osobních údajů však samozřejmě není jediným právním předpisem upravujícím práva a povinnosti osob v oblasti ochrany osobních údajů. Jak již bylo uvedeno výše, právo na ochranu osobnosti fyzických osob je zakotveno i v občanském zákoníku, a to v ustanoveních § 11 až 13, která umožňují dotčené osobě domáhat se subsidiárně svých práv v případech, kdy to není možné na základě Zákona, neboť se na danou situaci Zákon nevztahuje (např. v případě kamerového systému bez pořizování záznamu či nahodilého, resp. nikoli systematického zveřejnění osobních údajů)[17]. Problematikou nakládání s osobními údaji a jejich ochrany se dále částečně zabývá také například zákon č. 133/2000 Sb., o evidenci obyvatel, a mnoho dalších právních předpisů. V pracovněprávních vztazích je navíc problematika osobních údajů zaměstnanců či uchazečů o zaměstnání upravena také zákoníkem práce[18], zákonem o zaměstnanosti[19] či zákonem č. 251/2005 Sb., o inspekci práce[20].

---

[13] Dokument sub. pozn. č. 2.
[14] § 3 ZOOÚ
[15] § 2 ZOOÚ
[16] www.uoou.cz
[17] Morávek, J. *Ochrana osobních údajů v pracovněprávní agendě.* 1. vyd. Praha: BMSS Start, 2010, s. 14.
[18] Např. § 30 odst. 2, některá ustanovení § 105, § 312-314, § 316
[19] § 5 písm. a), §12 odst. 2, § 17, § 23, § 30 odst. 1 písm. d), § 32 odst. 2, § 102
[20] Např. § 4 odst. 4, § 8 písm. d) a j)

2. Osobní údaje

Jelikož Zákon o ochraně osobních údajů používá specifickou terminologii, je k pochopení právní úpravy ochrany osobních údajů nezbytné se s obsahem jednotlivých pojmů seznámit hned na počátku. Tyto pojmy bychom přitom mohli rozdělit do několika kategorií v závislosti na tom, jak s ochranou osobních údajů souvisí. Jedná se zejména o pojmosloví v oblasti předmětu ochrany (tj. co je chráněno - osobní údaje, citlivé údaje), komu tyto údaje patří (subjekt údajů), kdo s osobními údaji může nakládat (správce, zpracovatel a další osoby) a jakým způsobem se tak může dít (způsoby zpracování). V této a následující kapitole se proto budu zabývat obsahem a interpretací jednotlivých termínů, a to zejména s ohledem na výkladové ustanovení § 4 Zákona. Z pojmosloví Zákona pak vychází i další kapitoly této práce, věnované specifickým otázkám zpracování osobních údajů v pracovněprávních vztazích.

2.1 Osobní údaj

Termínem „osobní údaj“ rozumíme na základě ustanovení § 4 písm. a) Zákona jakoukoliv informaci či kombinaci informací týkající se subjektu údajů[21], na jejímž základě může být tento subjekt přímo či nepřímo identifikován. Určení, zda lze konkrétní údaj označit jako údaj osobní, je rozhodující pro správné posouzení, zda bude určitá informace a jednání s ní spojená (zejména zpracování) vůbec podléhat Zákonu[22]. Teprve po konstatování, že v daném případě lze tuto informaci klasifikovat jako osobní údaj, je osoba nakládající s touto informací povinna postupovat podle ustanovení Zákona.

Obsahově byla definice osobního údaje v Zákoně v podstatě převzata z čl. 2 písm. a) Směrnice a rovněž odpovídá vymezení tohoto pojmu v čl. 2 Úmluvy č. 108.

[21] K tomuto pojmu více viz bod 2.2 této kapitoly.
[22] Srov. Bartík, V. Janečková, E. *Zákon o ochraně osobních údajů s komentářem.* 1. vyd. Olomouc: ANAG, 2010, s. 32.

Definice osobního údaje v Zákoně se přitom skládá z několika charakteristik[23]. Předně se jedná o *informaci*, a to slovy Zákona jakoukoliv informaci – Zákon nestanoví požadavek, aby tato informace byla pravdivá či objektivní, v každém případě se však musí týkat *subjektu údajů*[24]. Dalším důležitým znakem této informace je, že může posloužit jako *nástroj identifikace* subjektu, k němuž se vztahuje. V rozličných situacích však tato schopnost identifikace nebude vždy stejná. Tak kupříkladu, na základě znalosti jména, příjmení a zaměstnavatele bude ve většině případů možné identifikovat konkrétní osobu, jelikož obvykle v jedné a téže společnosti více osob se stejným jménem i příjmením nepůsobí. Na druhou stranu, se znalostí jména, příjmení a města, ve kterém dotyčná osoba bydlí, se nám ve velkém množství případů osobu jednoznačně identifikovat nepodaří. Pokud však kupříkladu máme k dispozici iniciály jména a adresu konkrétní osoby, přičemž na dané adrese bydlí pouze jedna osoba s takovými iniciálami, bude se o osobní údaje jednat, neboť jejich znalost k identifikaci této osoby postačuje [25]. Osobními údaji však nejsou pouze typické identifikační znaky (např. jméno, příjmení, bydliště, datum narození), ale i další informace – kde se například dotyčná osoba pohybovala či s kým byla v kontaktu[26].

Při určení identifikovatelnosti je však dle odůvodnění Směrnice[27] třeba také přihlédnout ke všem prostředkům, které mohou být rozumně použity pro identifikaci dané osoby. O osobní údaj se tedy nebude jednat v těch případech, kdy zjištění identity subjektu údaje je sice možné, vyžadovalo by však nepřiměřené množství času, úsilí a materiálních prostředků. Jestliže však správce či jakákoliv jiná osoba může za vynaložení určité míry úsilí vytvořit přímou vazbu mezi údajem a jeho subjektem, bude se jednat o osobní údaj. Je ovšem třeba vzít v potaz i rychlost rozvoje technologických prostředků, které identifikovatelnost jednotlivce výrazně usnadňují, jakož i fakt, že nepřiměřené úsilí je zcela subjektivním

[23] Dokument sub. pozn. č. 22, s. 33.
[24] Tamtéž.
[25] Z rozhodovací činnosti ÚOOÚ – Pojem osobní údaj (čj. SPR-2904/08-3).
[26] Morávek, J. *Ochrana osobních údajů v pracovněprávní agendě.* 1. vyd. Praha: BMSS Start, 2010, s. 29.
[27] Recital 26

kritériem. Jestliže mají být konkrétní údaje uchovávány v rozsahu několika desítek let, dá se do jisté míry očekávat, že ačkoliv na jejich základě není možné osobu identifikovat dnes, v budoucnu se tato situace může velice snadno změnit[28].

Ve své definici zákon také hovoří o subjektu *určeném* a subjektu *určitelném*. V souvislosti s tím, co bylo uvedeno v předchozím odstavci, je možné o subjektu určeném hovořit tehdy, lze-li subjekt identifikovat v podstatě bez námahy. Na druhou stranu, není-li možné subjekt určit tzv. na první pohled, ale až po vynaložení určitého úsilí, budeme hovořit o subjektu určitelném.

K pojmu osobní údaj se již vícekrát vyjádřil také Nejvyšší správní soud, který při svém výkladu identifikovatelnosti jedince posuzuje zejména možnost danou osobu na základě zjištěných údajů určit a potažmo i kontaktovat. Za osobní údaj tak Nejvyšší správní soud nepovažuje např. znalost čísla občanského průkazu[29], neboť na základě této znalosti není možné konkrétní osobu určit, a to vzhledem neexistenci veřejného registru čísel občanských průkazů a také proměnlivosti tohoto údaje v čase. Na druhou stranu je třeba za osobní údaj považovat číslo mobilního telefonu, neboť využitím této informace se daná osoba bez dalšího stává určitelnou[30].

Souhrnně lze tedy říci, že pokud je možné k údaji přiřadit konkrétního jednotlivce a vytvořit tak vztah mezi údajem a subjektem tohoto údaje, hovoříme o údaji osobním (a potažmo o možnosti identifikovatelnosti subjektu). Bez existence takového vztahu se o osobní údaj jednat nebude, což ovšem nevylučuje možnost, že za změněných okolností by daný údaj mohl být k subjektu přiřazen a osobní údaj by se tak jednalo. Není tedy rozhodující, pro kolik příjemců je určitá informace osobním údajem, pakliže je tato informace s konkrétní osobou pro alespoň některé příjemce spojitelná[31].

[28] Dokument sub. pozn. č. 22, s. 35.
[29] Rozsudek NSS sp.zn. 1 As 98/2008 ze dne 29.7.2009.
[30] Rozsudek NSS sp.zn. 9 As 34/2008 ze dne 12.2.2009.
[31] Viz Výroční zpráva ÚOOÚ za rok 2010, s. 42.

Jako protipól pojmu osobní údaj pak Zákon[32] uvádí pojem anonymní údaj, neboť teprve poté, co jsou určité údaje anonymizovány a je tak nenávratně znemožněno přiřadit je k jednotlivým subjektům, tyto údaje zaručeně přestávají být údaji osobními. Často se nicméně pojmem anonymizace označuje postup, při němž jsou konkrétní identifikátory (nejčastěji jméno a příjmení v kombinaci s datem narození) nahrazeny vygenerovaným číselným kódem. Obvykle však zůstává převodní algoritmus správci údajů znám a obráceným postupem je tak možné konkrétní subjekt znovu zpětně identifikovat. Správně by proto tento postup měl být označován jako „pseudoanonymizace“, neboť subjekt „anonymizovaného“ údaje není neidentifikovatelný ve vztahu ke všem osobám (minimálně správce je identifikace schopen) a schopnost identifikace subjektu tak zůstává zachována.

2.2 Subjekt údajů

Subjektem osobních údajů je osoba, k níž se tyto údaje vztahují. Jak plyne již ze samotné zákonné definice (§ 4 písm. d) Zákona), subjektem údajů může být výhradně fyzická osoba, a to proto, že instituty jako jsou ochrana soukromí či *lidská* důstojnost, mohou pojmově souviset pouze s osobami fyzickými ve vztahu k jejich soukromé sféře. Z tohoto důvodu nemůže také být subjektem údajů právnická osoba[33] ani fyzická osoba podnikající za předpokladu, že se údaje týkají jejího podnikání a nezasahují tedy oblast jejího soukromého života, a to ani za použití analogie[34].

2.3 Citlivý údaj

K subjektu údajů se však nevztahují pouze „obyčejné“ osobní údaje, nýbrž i jejich zvláštní podkategorie – údaje citlivé. Jako citlivé údaje označujeme ty z osobních údajů, které, bude-li jejich subjekt identifikován, umožňují poměrně

[32] § 4 písm. c) ZOOÚ
[33] Toto bylo rovněž potvrzeno rozsudkem Nejvyššího správního soudu sp.zn. 6 A 83/2001 ze dne 13.10.2004.
[34] Dokument sub. pozn. č. 22, s. 44.

velké narušení soukromé sféry subjektu[35]. Zákonná definice v ustanovení § 4 písm. d) Zákona opět vychází ze znění Směrnice, která, přestože tento pojem v čl. 2 nedefinuje, hovoří v čl. 8 o zpracování zvláštních kategorií údajů, a to takových, které odhalují rasový či etnický původ, politické názory, náboženské nebo filozofické přesvědčení, odborovou příslušnost či údaje týkající se zdraví a sexuálního života. Obdobně je tato subkategorie osobních údajů definována v čl. 6 Úmluvy č. 108, která do ní navíc zahrnuje údaje týkající se odsouzení za trestný čin. Zákonná definice byla v porovnání s výše uvedenými výčty navíc rozšířena o údaje vypovídající také o národnosti (nikoliv státní příslušnosti[36]) subjektu a biometrické údaje umožňující přímou identifikaci nebo autentizaci subjektu údajů (ne tedy všechny biometrické údaje jsou údaji citlivými). V důsledku osobní povahy těchto informací jsou proto pro jejich zpracování stanoveny přísnější podmínky, než pro zpracování většiny osobních údajů[37].

Jak vyplývá ze zákonného znění definice citlivých údajů, jedná se v případě politických či filozofických a náboženských údajů o „názory". Není tedy možné rozsah pojmu citlivý údaj v této oblasti zúžit pouze na příslušnost vůči politické straně, církvi či jiné náboženské organizaci, naopak je potřeba do něj zahrnout také náklonnost k určitým skupinám, názory či vztah k víře. Citlivým údajem tak kupříkladu bude to, jakou politickou stranu subjekt údajů volil[38].

Z hlediska pracovního práva je jistě významné, že mezi skupinu citlivých údajů je zahrnuta také informace o členství v odborových organizacích, neboť se i v tomto případě jedná o vnitřní postoj a názory člověka, na jejichž základě se však velice snadno může daný subjekt stát předmětem nerovného zacházení, a to nejen ze strany zaměstnavatele současného, nýbrž i potenciálního, či dokonce ze strany spolupracovníků. I zde je navíc na místě extenzivní výklad, a proto je pod pojmem

[35] Srov. Morávek, J. *Ochrana osobních údajů v pracovněprávní agendě.* 1. vyd. Praha: BMSS Start, 2010, s. 16; nebo dokument sub. pozn. č. 22, s. 37.
[36] Státní příslušník České republiky se v podstatě může hlásit k libovolné národnosti, byť tak nejčastěji činí v poměru k národnosti české, moravské nebo slezské.
[37] K citlivým údajům jako jsou odsouzení za trestný čin a informace o zdravotním stavu či údaje biometrické a genetické více viz subkapitoly 6.3 a 7.1.6.
[38] Dokument sub. pozn. č. 22, s. 38.

„členství v odborových organizacích“ nezbytné rozumět také členství či podporu jakéhokoliv sdružení (i bez právní subjektivity), jehož cílem je ochrana a prosazování práv zaměstnanců v pracovněprávních vztazích[39]. Na druhou stranu však zákoník práce na mnoha místech[40] předpokládá znalost zaměstnavatele o tom, kteří zaměstnanci jsou členy odborové organizace či přímo jejích orgánů, resp. členy rady zaměstnanců, a je tedy otázkou, jak má zaměstnavatel v těchto případech postupovat. Zaměstnavatelé by tak zřejmě tyto informace neměli sami aktivně zjišťovat a vyčkat, bude-li jim poskytnuta ze strany dotyčného zaměstnance (obvykle při uplatňování práv s tím souvisejících). Neuplatní-li tuto skutečnost zaměstnanec sám, nemá zaměstnavatel povinnost k němu přistupovat jako k členovi organizace zastupující zaměstnance.

2.4 Správce, zpracovatel, příjemce

2.4.1 Správce

Správcem osobních údajů se zásadně může stát kdokoliv bez ohledu na to, zda se jedná o fyzickou či právnickou osobu, státní nebo jiný orgán, a to vzhledem k vymezení působnosti Zákona v jeho ustanovení § 3 odst. 1. Výjimku představují fyzické osoby za předpokladu, že osobní údaje zpracovávají výhradně pro vlastní potřebu či osoby shromažďující osobní údaje pouze nahodile (§ 3 odst. 3 a 4 Zákona). Důležitým znakem pro odlišení fyzické osoby v postavení správce tak je skutečnost, že osobní údaje nezpracovává výlučně pro vlastní potřebu, ale za určitým konkrétním cílem (kterým bude často dosažení zisku, ať již přímo či zprostředkovaně). Mezi zákonné znaky správce tak Zákon[41] řadí mimo jiné i skutečnost, že právě správce určuje účel a prostředky zpracování osobních údajů. Z této definice vyplývá také první z mnoha omezení zpracování osobních údajů, které budou později zmíněny, a to skutečnost, že osobní údaje není dovoleno zpracovávat bez stanovení účelu (tzn. pro případ, že by se v budoucnu mohl

[39] Tamtéž.
[40] Srov. § 61 odst. 2 ZP, § 203 odst. 2 písm. a) ZP nebo § 286 odst. 2 ZP.
[41] § 4 písm. j) ZOOÚ

objevit důvod pro jejich využití) ani je využívat k jinému účelu, než ke kterému je jejich zpracování určeno. Charakteristikou osoby správce se zabýval i Nejvyšší správní soud a zdůraznil, že správcem bude vždy právě ta osoba, která stanoví zejména účel a prostředky zpracování osobních údajů. I kdyby osoba byla původně v jiném postavení ve vztahu ke zpracování osobních údajů (např. zpracovatelem), v okamžiku, kdy sama začne stanovovat účel zpracování, dostane se do pozice správce. Tímto způsobem je tak zaručena efektivní ochrana při zpracovávání osobních údajů, neboť práva a povinnosti správce bude mít zpracovávající osoba bez ohledu na své formální označení[42].

Mezi další znaky správce patří také fakt, že správce zpracování osobních údajů aktivně provádí (tím však může pověřit také jinou osobu) a neoddělitelně také skutečnost, že za zpracování osobních údajů v každém případě odpovídá, a to buď sám anebo společně a nerozdílně další osobou (zpracovatelem)[43].

2.4.2 Zpracovatel

Zpracovatelem se podle ustanovení § 4 odst. k) Zákona rozumí každý, kdo osobní údaje zpracovává, a to na základě zákona nebo pověření správce. Na rozdíl od správce tak zpracovatel údaje zpracovává nikoli na základě pouhého vlastního rozhodnutí, ale teprve na základě pověření ze strany správce (slovy Směrnice „*pro* správce“) či právního předpisu. Samostatně také provádí pouze zpracování, aniž by však určoval jeho způsob a prostředky. Pojmově tedy není možné, aby jedna a táž osoba byla správcem a zpracovatelem současně, neboť činnost správce již činnosti zpracovatele v sobě zahrnuje. Za zpracovatele však není považován zaměstnanec správce, neboť v takovém případě se fakticky nejedná o osobu od správce odlišnou.

Naproti tomu však může existovat vůči týmž osobním údajů vztah dvou správců. Zpracovatel se také může u určitého zpracování stát sekundárně

[42] Srov. dokument sub. pozn. č. 30.
[43] Dokument sub. pozn. č. 22, s. 57.

správcem, a to kupříkladu tehdy, když stanoví i jiný, svůj vlastní účel zpracování (za předpokladu dodržení zákonných náležitostí, zejména získání souhlasu původního správce a většinou také samotného subjektu údajů).

Nejčastěji ke vzniku pověření zpracováním ze strany správce dochází na smluvním základě. V takovém případě je správce povinen uzavřít se zpracovatelem dle ustanovení § 6 Zákona písemnou smlouvu o zpracování. Ve smlouvě správce stanoví, v jakém rozsahu a za jakým účelem je zpracovatel povinen údaje zpracovávat, přičemž zpracovatel se současně musí zavázat tyto údaje náležitě zabezpečit. Aby se nejednalo o pouhou deklaraci závazku zabezpečit údaje, je zpracovatel povinen uvést přímo ve smlouvě konkrétní opatření, s jejichž pomocí budou údaje zabezpečeny[44]. Na základě dohody by si také správce mohl ve smlouvě o zpracování vyhradit právo kontroly, jak jsou u zpracovatele konkrétní bezpečnostní opatření dodržována. Absence jednoho či více zákonných požadavků ve smlouvě o zpracování by sice nezpůsobila její absolutní neplatnost, nicméně by se v důsledku toho nejednalo o smlouvu dle § 6 Zákona, a zpracovatel by tak nakládal s osobními údaji neoprávněně (tj. ani na základě zákona ani na základě smlouvy ve smyslu § 6 Zákona, která musí být písemná) a spolu se správcem by se tak vystavoval hrozbě udělení sankce ze strany Úřadu podle Hlavy VII. Zákona[45].

Kromě zákonných náležitostí může smlouva obsahovat i další ujednání smluvních stran podrobněji vymezující jejich vzájemná práva a povinnosti. Tak kupříkladu může správce využít možnosti, kterou mu dávají ustanovení § 11 odst. 7 nebo § 12 odst. 4 Zákona a přenést na zpracovatele některé ze svých povinností při zpracování údajů. Zákon nicméně nevyžaduje, aby smlouva o zpracování tvořila separátní dokument[46]. Může tak být součástí širšího smluvního ujednání, jakou může být a velice často i bývá pověření třetího subjektu vedením určité výsekové agendy (outsourcing). U zaměstnavatelů bývá nejčastěji outsourcována oblast personální a mzdové agendy či zajišťování služeb v oblasti IT.

[44] Dokument sub. pozn. č. 22, s. 113
[45] Tamtéž.
[46] Tamtéž.

Jak uvádí Úřad ve svém stanovisku č. 1/2009[47], zejména v případě zpracování osobních údajů velkými společnostmi dochází k tzv. řetězení zpracovatelů. O tuto situaci se jedná v případě, kdy ani sám zpracovatel není schopen či nemá zájem poskytovat správci veškeré zpracovatelské činnosti, a proto jejich provedením pověří další subjekt – dílčího zpracovatele (např. prostřednictvím subdodávky, kterou zpracovatel pověří svou dceřinou společnost). Pojmově však smlouva o zpracování může být uzavřena pouze mezi správcem a zpracovatelem, nikoli mezi dvěma zpracovateli[48]; začlenění dalšího článku do zpracovatelského řetězce je ovšem možné s využitím ustanovení § 14 Zákona, který umožňuje, aby jak správce, tak zpracovatel zajistili zpracování prostřednictvím svých zaměstnanců či dalších osob (fyzických i právnických). Tyto osoby však nebudou v postavení zpracovatele a nebude s nimi uzavřena smlouva o zpracování ve smyslu § 6 Zákona. Rozhodnutí o zapojení dalšího subjektu do zpracovatelského řetězce také nemůže zpracovatel učinit bez souhlasu správce, neboť i během zpracování osobních údajů dalšími osobami je to právě správce, kdo je zodpovědný za zajištění bezpečného nakládání s osobními údaji, a není přípustné, aby tento nad nimi ztratil svou kontrolu[49].

2.4.3 Příjemce

Vedle správce a zpracovatele mohou s osobními údaji přijít do styku i další osoby, tzv. příjemci. Na základě ustanovení § 4 písm. o) Zákona je příjemcem ten, komu jsou osobní údaje jednorázově zpřístupněny a kdo s nimi již nadále systematicky nepracuje, a tedy je ani nijak nezpracovává, resp. jeho oprávnění ke zpracování není odvozeno od oprávnění správce, který mu údaje zpřístupnil (na rozdíl od postavení zpracovatele[50]). Tato definice se však nevztahuje na orgány, kterým jsou údaje zpřístupněny v rámci zvláštního šetření. Fakticky se sice

[47] Stanovisko ÚOOÚ č. 1/2009 – Zpracování osobních údajů na základě smluv uzavíraných se zpracovateli (tzv. řetězení zpracovatelů osobních údajů).
[48] Dokument sub. pozn. č. 22, s. 58.
[49] Dokument sub. pozn. č. 47.
[50] Kučerová, A. Nonnemann, F. *Ochrana osobních údajů v otázkách a odpovědích.* 1. vyd. Praha: BOVA POLYGON, 2010, s. 44.

v takovém případě o příjemce jednat bude, správce údajů však bude osvobozen od některých (s příjemcem souvisejících) povinností ve vztahu k subjektu údajů (např. informování subjektu dle § 12 Zákona)[51]. Příkladem „obyčejného“ příjemce osobních údajů může být mimo jiné i personální agentura, která osobní údaje uchazeče předá potenciálnímu zaměstnavateli, aby sám na jejich základě zhodnotil, zda nabídne uchazeči absolvování přijímacího pohovoru. Personální agentura je přitom povinna uchazeče o zaměstnání již při získávání jeho osobních údajů informovat o skutečnosti, že tyto údaje mohou být předány třetím osobám (dle mého názoru v tomto případě postačí obecná informace, že osobní údaje mohou být zpřístupněny třetím osobám – potenciálním zaměstnavatelům[52]).

[51] Dokument sub. pozn. č. 22, s. 66.
[52] Srov. dokument sub. pozn. č. 50, s. 40.

3. Zpracování osobních údajů

Stejně jako pojmy v předchozí kapitole týkající se předmětu zpracování, jakož i osob, které údaje zpracovávají, vychází i obsah termínu samotného zpracování osobních údajů především z ustanovení § 4 Zákona, neboť ten ve svém písmenu e) stanoví, že zpracováním osobních údajů se rozumí jakákoliv operace, kterou správce nebo zpracovatel s osobními údaji provádí. Především se tak (slovy Zákona) jedná o jejich shromažďování, zpřístupňování, předávání, zveřejňování, uchovávání, likvidaci a další činnosti. Konkrétnější naplň některých z těchto operací je potom vymezena pod následujícími písmeny ustanovení § 4 Zákona.

Hned v úvodu dané definice zpracování Zákon vymezuje, že zpracováním se rozumí jakákoliv operace či soustava operací (Směrnice ve svém čl. 2 písm. b) hovoří o úkonech či souborech úkonů). Je tedy jasně stanoveno, že i jediný samostatný úkon týkající se osobních údajů je již jejich zpracováním. Musí se ovšem jednat o úkon systematický (jak zde již bylo zmíněno výše, správcem není ten, kdo osobní údaje *shromažďuje* pouze nahodile). Dle mého názoru však správcem nebude ve smyslu Zákona ani ten, kdo osobní údaje zpracuje nahodile i jinak než formou jejich shromáždění, k čemuž dospívám výkladem a contrario právě k ustanovení § 4 písm. e) první věta. O zpracování údajů se však za výše uvedených předpokladů bude jednat bez ohledu na to, zda k němu bude docházet manuálně či automatizovaně (v podstatě tedy jakkoliv)[53].

Na rozdíl od znění Zákona neobsahuje definice zpracování uvedená ve Směrnici osobu správce či zpracovatele. Obsah termínu „zpracování“ však je v obou případech stejný, neboť není pojmově možné, aby osobní údaje zpracovával ve smyslu Zákona či Směrnice někdo jiný než správce či zpracovatel – a to bez ohledu na to, zda si je tohoto svého postavení vědom.

[53] Viz Bartík, V. Janečková, E. *Zákon o ochraně osobních údajů s komentářem.* 1. vyd. Olomouc: ANAG, 2010, s. 45.

Se zpracováním jako takovým úzce souvisí také povinnost správce zpracovávat pouze přesné osobní údaje, což zahrnuje i požadavek jejich pravdivosti, a to alespoň v takové míře, v jaké je možné pravdivost údajů zjistit[54] (tato povinnost je přitom jednou z nejčastěji porušovaných povinností ze strany správců[55]). V souvislosti s tím ukládá Zákon správcům povinnost osobní údaje aktualizovat, přičemž frekventovanost aktualizací ponechává na uvážení správce. Jestliže správce zjistí, že jím zpracovávané údaje jsou nepřesné, má povinnost je blokovat (tj. zamezit jejich dalšímu zpracování), a poté buď opravit či zlikvidovat. Výjimku umožňující zpracovávat osobní údaje bez ohledu na jejich přesnost a pravdivost poskytuje správcům pouze ustanovení § 3 odst. 6 Zákona (je-li to nezbytné pro zajištění bezpečnosti či obrany ČR, vnitřního pořádku apod.)[56].

Obsah výše uvedeného pojmu *blokování* je opět vymezen ve výkladovém ustanovení § 4 Zákona, a to pod písmenem h). I blokování údajů je tak jedním ze způsobů zpracování údajů spočívající ve znemožnění přístupu k údajům po určitou dobu tak, aby jedinými oprávněnými osobami k přístupu k údajům byl jejich subjekt, správce a popřípadě i zpracovatel. Správce a zpracovatel však svého přístupu mohou využít pouze omezeně, a to zejména právě k aktualizaci, opravě či likvidaci údajů[57].

K aktualizaci údajů může dojít na základě zjištění ze strany správce, ale také v souvislosti s podnětem ze strany samotného subjektu, neboť jedním z práv subjektu ve vztahu k vlastním osobním údajům je i právo domáhat se opravy nepřesných údajů[58]. V pracovněprávních vztazích bývá obvyklé, že pracovní či obdobná smlouva obsahuje ustanovení, na jehož základě je zaměstnanec povinen zaměstnavateli bezodkladně či do určité doby sdělit veškeré změny osobních údajů, které zaměstnanec na počátku či před vznikem pracovního, resp. obdobného vztahu zaměstnavateli poskytl, aby tak zaměstnavatel mohl dostát své povinnosti

[54] § 5 odst. 1 písm. c) ZOOÚ
[55] Viz dokument sub. pozn. č. 53, s. 72.
[56] Kolman, P. Správní sankce na úseku ochrany osobních údajů. *Právní rádce*. 2009, č. 10, s. 40.
[57] Viz dokument sub. pozn. č. 53, s. 73.
[58] Na základě ust. § 21 odst. 1 písm. b) ZOOÚ.

správce zpracovávat přesné a pravdivé osobní údaje svých zaměstnanců. Dle mého názoru lze tento mechanismus požadovat za dostatečný, aby zaměstnavatel dostál své povinnosti zpracovávat pouze přesné a aktuální osobní údaje[59].

Protože o jednotlivých způsobech a prostředcích zpracování bude blížeji pojednáno také v následujících kapitolách, kromě následujících třech způsobů se jimi v této kapitole více zabývat nebudu.

3.1 Shromažďování

Jak již bylo uvedeno výše, shromažďování patří mezi způsoby zpracování osobních údajů. I u definice shromažďování[60] Zákon zdůrazňuje, že se musí jednat o shromažďování systematické, aby bylo možné aplikovat ZOOÚ. I přes opakované užití pojmu *systematický* však Zákon jeho přesný výklad nepodává. Bude se tak patrně jednat o jakékoliv zpracování (tedy nejen shromažďování), které správce a další osoby činí s cílem tyto údaje jakkoliv využít, byť se nemusí jednat o činnost nepřetržitou[61]. Zjednodušeně, správce se s údaji neseznámil náhodou, nýbrž proto, že tak sám chtěl, k čemuž měl a má vlastní důvod. Nasvědčuje tomu i další ze znaků shromažďování, jímž je skutečnost, že k němu dochází za účelem budoucího zpracování. Vzhledem k tomu, že zpracováním je nutno rozumět i likvidaci údajů, bude se tak ZOOÚ vztahovat i na ty správce, kteří osobní údaje subjektů nejprve shromáždí, ale poté od jejich dalšího zpracování upustí a zlikvidují je.

Zákon dále stanoví, že cílem shromažďování údajů je jejich získání za účelem dalšího uložení pro jejich okamžité nebo pozdější zpracování. Již před započetím shromažďování údajů by si však měl být správce vědom, k jakému účelu bude jejich pozdější zpracování sloužit. Údaje jsou přitom ukládány na „nosič informací“, jímž však může být prakticky cokoli (v dnešní době přichází

[59] Srov. Z rozhodovací činnosti ÚOOÚ – K problematice aktualizace zpracovávaných osobních údajů (čj. 10/06/SŘ-OSČ, 13/06/SŘ-OSČ, 31/06/SŘ-OSČ).
[60] § 4 písm. f) ZOOÚ
[61] Srov. dokument sub. pozn. č. 53, s. 45.

kromě tradičních nosičů v úvahu zejména úložiště digitálních dat umožňující dlouhodobé zachování údajů v trvalé kvalitě); k dalšímu zpracování přitom může dojít okamžitě, nebo i později. Důležitým znakem shromažďování údajů, které má podléhat Zákonu však je skutečnost, že možnost dalšího zpracovávání nashromážděných údajů zůstává správci otevřena[62].

3.2 Uchovávání

Uchováním jsou osobní údaje udrženy v takové podobě, která umožňuje jejich další zpracování[63]. Možnost dalšího zpracování však bude do značné míry závislá na charakteru a odolnosti nosiče informací, na nějž byly údaje po shromáždění uloženy. Pokud to nosič informací umožňuje, je navíc možné vytvářet jeho kopie, s jejichž pomocí může docházet ke zpracování údajů více zpracovateli najednou. Je však nutné si uvědomit, že ačkoliv obecně nikdy kopie nedosahuje hodnoty originálu, i ona bude obsahovat osobní údaje (za předpokladu, že se nebude jednat o natolik nekvalitní kopii, ze které osobní údaje nebude již možné znovu získat), a proto bude nezbytné s ní zacházet jako s jakýmkoli jiným (i původním) nosičem údajů.[64]

S uchováváním údajů úzce souvisí i povinnost správce stanovená v ustanovení § 5 odst. 1 písm. e), která správce opravňuje uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování, a také povinnost stanovená v ustanovení témže odstavci písm. h), tj. nesdružovat osobní údaje, které byly získány k rozdílným účelům[65]. Spojením vícera osobních údajů týkající se téhož subjektu by totiž mohlo dojít k situaci, kdy vznikne informace zcela jedinečná s vysokou vypovídající hodnotou o subjektu, a to zcela bez vědomí subjektu. Správce si sice může osobní údaje zpracovávané za různými účely uchovávat za použití stejných prostředků, nesmí je však při tom sdružovat[66]. Jako

[62] Srov. dokument sub. pozn. č. 53, s. 49.
[63] § 4 písm. g) ZOOÚ
[64] Viz dokument sub. pozn. č. 53, s. 50.
[65] Srov. dokument sub. pozn. č. 53, s. 52.
[66] Srov. dokument sub. pozn. č. 53, s. 84.

uchovávání v souladu se zákonem si tak lze v praxi představit uložení na samostatných lokálních sítích či oddělených samostatně spravovaných uživatelských účtech, resp. ve fyzické podobě v oddělených složkách[67].

Ve vztahu k uchovávání zaměstnavatelé často stojí před otázkou, jak dlouho tedy mají osobní údaje svých zaměstnanců uchovávat, a to zejména po skončení pracovního poměru[68]. Chybou přitom bývá všechny údaje ihned zlikvidovat v obavě, že by se společnost mohla dopustit porušování právních předpisů, jakož i situace opačná, kdy zaměstnavatel uchovává veškeré údaje bývalých zaměstnanců dlouhá léta po skončení jejich pracovního poměru. Správným řešením v této situaci je následující postup: provedení kategorizace údajů do jednotlivých skupin v návaznosti na to, zda a jak dlouhou dobu jejich uchovávání stanoví zvláštní předpis (např. pro účely důchodového a sociálního zabezpečení či účely daňové) a jejich rozdělené uchovávání podle účelu. Zbylé údaje by měl zaměstnavatel uchovávat po dobu, během níž je může potřebovat k uplatnění či naopak popření nároků bývalého zaměstnance, tj. během obecné promlčecí doby dle občanského zákoníku v délce tří let[69]. Přestože ÚOOÚ upozorňuje, že paušalizovat délku uchování ostatních údajů odkazem na obecnou promlčecí či prekluzivní dobu je chybné[70], obávám se, že požadavek další selekce těchto údajů a posouzení, které mohou být během promlčecí doby uchovávány a které naopak již nebudou účelné, by správce spíše vedlo k likvidaci všech údajů a v případě pozdějšího soudního sporu jim značně ztížil jejich důkazní situaci.

[67] Matoušová, M. a kol. *Ochrana osobních údajů v otázkách a odpovědích*. 1. vyd. Praha: ASPI Publishing, 2004, s. 49.
[68] Morávek, J. *Ochrana osobních údajů v pracovněprávní agendě.* 1. vyd. Praha: BMSS Start, 2010, s. 52.
[69] Viz také dokument sub. pozn. č. 68, jakož i Z rozhodovací činnosti ÚOOÚ – Ke zpracování osobních údajů bývalých zaměstnanců (čj. SKO-2077/07).
[70] Srov. Z rozhodovací činnosti ÚOOÚ – Ke zpracování osobních údajů bývalých zaměstnanců (čj. SKO-2077/07).

3.3 Zveřejnění

I zveřejněním osobních údajů dochází k jejich zpracování. Samotná definice tohoto pojmu[71] hovoří o zveřejnění jako o formě *zpřístupnění*, a to zejména prostřednictvím hromadných sdělovacích prostředků (v dnešní době také často prostřednictvím internetu), na jejichž základě dochází ke zpřístupnění údajů širokému okruhu příjemců. Pod „obyčejným" zpřístupněním údajů pak chápeme jejich zpřístupnění omezenému okruhu adresátů, byť ani jejich počet nemusí být nejnižší. Zpřístupnění údajů prostřednictvím médií (tj. zveřejnění) však v dnešní době znamená jejich zpřístupnění prakticky komukoli.[72] Také zveřejnění, má-li podléhat působnosti Zákona, však musí být vykládáno s ohledem na definici zpracování, a tedy k němu musí docházet systematicky. Ne na všechny případy zveřejnění se tak Zákon bude vztahovat.

Zveřejněním osobních údajů na internetu se však zabýval také Evropský soudní dvůr ve svém rozsudku C-101/01 ze dne 6.11.2003, který zaujal ve vztahu ke zpracování osobních údajů poměrně extenzivní výklad. V daném případě umístila švédská občanka paní Lindqvist na svou webovou stránku příspěvek, který obsahoval osobní údaje některých jejich kolegů včetně telefonních čísel, aniž by k tomu měla souhlas dotčených osob. Na základě žádosti jednoho z kolegů však tento příspěvek ihned odstranila. Švédský úřad na ochranu osobních údajů jí i přesto uložil pokutu za neoprávněné zpracování osobních údajů; proti tomuto rozhodnutí se paní Lindqvist odvolala. Na základě předběžné otázky švédského soudu pak Evropský soudní dvůr shledal, že umístění osobních údajů na internet skutečně představuje jejich zpracování, a to i v rámci neziskové sféry. Na jednání paní Lindqvist nelze totiž uplatnit výjimku podle čl. 3 odst. 2 Směrnice, neboť se nejedná o zpracování prováděné pro výkon výlučně osobních či domácích činností – údaje byly na internetu přístupné širokému okruhu veřejnosti. Soud rovněž odmítl i argument paní Lindqvist, že bylo rozhodnutím úřadu omezeno její právo na svobodu projevu, a vyjádřil se také k otázce, zda umístění osobních údajů na

[71] § 4 písm. l) ZOOÚ

internet představuje jejich předávání do třetích zemí; v této souvislosti dospěl k závěru, že se o předávání údajů do třetích zemí nejedná za předpokladu, že údaje nejsou přímo zasílány uživatelům v těchto zemích a že se server, na němž je webová stránka umístěna, nenachází ve třetí zemi (byť je stránka s údaji samozřejmě přístupná i z těchto zemí) [73].

[72] Viz dokument sub. pozn. č. 53, s. 59.
[73] Srov. body 27, 47, 48, 71 a 78 rozsudku Evropského soudního dvora C-101/01 ze dne 6.11.2003.

4. Práva subjektu údajů

V předchozích kapitolách bylo vymezeno, co jsou osobní údaje a jejich zpracování, jakož i osoby, které je zpracovávají. Nyní se proto dostáváme k právům subjektu údajů, neboť cílem právní úpravy ochrany osobních údajů je garance jejich práv a to zejména v podobě stanovení základních podmínek (povinností) pro nakládání s osobními údaji, která mají ochranu a vymahatelnost práv subjektů ve vztahu k vlastním osobním údajům zaručit.

Subjekty, tj. fyzické osoby, k nimž se dané osobní údaje vztahují, mají především právo na ochranu svých osobních údajů. Od jednotlivých konkrétních práv a oprávnění subjektů, jimiž je ochrana jejich údajů zabezpečována, se přitom zrcadlově odvíjí povinnosti správce a dalších osob při jejich zpracovávání, o nichž bude pojednáno v následující kapitole. S každou povinností při zpracování osobních údajů tak souběžně existuje právo subjektu domáhat se jejího splnění. Níže uvedená práva subjektů v souvislosti se zpracováním jejich osobních rozhodně nepředstavují taxativní výčet práv subjektů; jedná se o ta nejdůležitější práva, kterých by si každý subjekt údajů měl být vědom a aktivně se jich domáhat, má-li být v právních vztazích garantována minimální úroveň ochrany osobních údajů.

4.1 Souhlas subjektu údajů

Podmínka subjektu osobních údajů s jejich zpracováváním představuje jednu ze základních premis nakládání s osobními údaji; vychází přitom ze zásady, podle níž právo disponovat s osobními údaji náleží fyzické osobě, k níž se tyto údaje vztahují, a nikoli tomu, kdo je zpracovává[74]. Správce tak může zpracovávat osobní údaje subjektů zásadně s jejich souhlasem, nestanoví-li zákon jinak[75]. I při použití takovéto zákonné výjimky (tj. absence nutného souhlasu) tím však není dotčena

[74] Srov. rozsudek NSS čj. 9 As 34/2008 ze dne 12.02.2009.
[75] § 5 odst. 2 ZOOÚ

informační a poučovací povinnost správce stejně jako právo subjektu na ochranu svého soukromého a osobního života.

Souhlas jako takový je vymezen již ve výkladovém ustanovení § 4 Zákona, a to konkrétně § 4 písm. n), které stanoví, že se musí jednat o svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu ke zpracování svých osobních údajů. Souhlas tedy naplňuje znaky jednostranného právního úkonu[76], a proto je zapotřebí jeho „kvalitu" hodnotit podle obecných náležitostí právních úkonů stanovených v § 37 an. ObčZ: aby byl právní úkon platný, musí být učiněn svobodně a vážně, určitě a srozumitelně.

V souladu s definicí obsaženou v Zákoně musí být souhlas se zpracováním osobních údajů také svobodný a vědomý. Podmínka vědomosti se přitom odráží v informační povinnosti správce[77], neboť aby mohl být souhlas subjektu vědomý, musí mít subjekt k dispozici dostatek informací o tom, co se vlastně bude s jeho osobními údaji dít a za jakých podmínek je souhlas udělován. Požadavek vědomého souhlasu většinou nepředstavuje zásadní překážku způsobující nedostatky v charakteru a „kvalitě" poskytnutého souhlasu, to však již neplatí o podmínce jeho svobodného udělení. V pracovněprávních vztazích může svobodnost udělení souhlasu představovat problém vzhledem ke slabší pozici zaměstnance vůči zaměstnavateli, neboť zaměstnanec často ve skutečnosti nemá možnost souhlas se zpracováním svých osobních údajů odepřít, aniž by tím neutrpěl újmu (nejčastěji se jedná o skrytou újmu spočívající například v tom, že je se zaměstnancem nadále zacházeno jako s „potížistou", a to nejen ze strany zaměstnavatele, ale i ostatních kolegů). Rovněž i Stanovisko Pracovní skupiny 29[78] č. 48 k této problematice uvádí, že v pracovněprávních vztazích by se zpracování

[76] Na souhlas je vždy zapotřebí nahlížet právě jako na jednostranný právní úkon subjektu, a to bez ohledu, zda je vyjádřen samostatně či jako součást dvoustranného úkonu, kterým obvykle bývá konkrétní smlouva. Viz též Bartík, V., Janečková, E. *Zákon o ochraně osobních údajů s komentářem.* 1. vyd. Olomouc: ANAG, 2010, s. 65.
[77] Upravené v § 5 odst. 4, § 11 a § 12 ZOOÚ.
[78] Skupina zřízená na základě článku 29 Směrnice jako poradní orgán v souvislosti s problematikou ochrany osobních údajů a soukromí. Skupina je složena z vedoucích kontrolních úřadů na ochranu osobních údajů v jednotlivých členských zemích.

osobních údajů na základě souhlasu mělo zásadně omezit na situace, kdy má zaměstnanec skutečně svobodnou volbu s postupem zaměstnavatele nesouhlasit a reálnou možnost svůj souhlas následně bez jakýchkoliv následků odvolat. V situaci, kdy má zaměstnanec svobodnou volbu značně ztíženou zejména s vědomím potenciálních následků v případě neudělení souhlasu, nelze ani již udělený souhlas považovat za platný právní úkon[79].

Poslední podmínku udělení bezvadného souhlasu se zpracováním osobních údajů pak obsahuje ust. § 5 odst. 4 v první větě – při udělení souhlasu musí být subjekt současně informován o tom, pro jaký účel zpracování a k jakým osobním údajům, jakému správci a na jaké období je souhlas dáván[80]. Podrobněji bude k této náležitosti pojednáno v následující kapitole v části týkající se informační povinnosti správce.

S výjimkou zpracování citlivých údajů nemusí však být souhlas udělen výslovně; postačí tedy i jeho konkludentní udělení, a to například tím, že subjekt své údaje správci na jeho žádost poskytne, samozřejmě za předpokladu splnění ostatních náležitostí (tj. zejména informovanosti souhlasu)[81]. Zákon sám nevyžaduje poskytnutí písemného souhlasu, avšak vzhledem k prokazovací povinnosti správce stanovené v § 5 odst. 4 druhá věta ústně udělený souhlas nebude pro správce příliš praktický, neboť se v případě potřeby prokázání skutečnosti, že byl souhlas subjektem udělen, ocitne v důkazní nouzi. Ke konkludentnímu (nicméně písemnému) udělení souhlasu však dochází například v případech, kdy uchazeč o zaměstnání sám od sebe zasílá společnostem svůj životopis a v průvodním dopise žádá o zařazení do databáze uchazečů. V takových případech samozřejmě není nutné žádat subjekt dodatečně o poskytnutí souhlasu se zpracováním jeho údajů, neboť subjekt jej již dostatečně vyjádřil tím, že své údaje správci sám zaslal. Tuto situaci je také možné podřadit pod zákonnou výjimku

[79] Viz také rozhodnutí ÚOOÚ zn. 56/06/SŘ nebo Stanovisko WP 48 o zpracování osobních údajů v souvislosti se zaměstnáváním.
[80] Srov. Morávek, J. *Ochrana osobních údajů v pracovněprávní agendě.* 1. vyd. Praha: BMSS Start, 2010, s. 43.

stanovenou v § 5 odst. 2 písm. b), kdy lze údaje zpracovávat bez souhlasu subjektu (viz dále).

Specifické podmínky souhlasu ke zpracování citlivých údajů obsahuje § 9 písm. a) Zákona, přičemž základní odlišností od požadavků stanovených na udělení souhlasu se zpracováním ostatních osobních údajů představuje podmínka výslovnosti. Dle mého názoru požadavek výslovnosti však neznamená, že by souhlas musel být za každých okolností udělen písemně (přestože to lze vzhledem k prokazovací povinnosti správců maximálně doporučit), ale představuje skutečnost, že subjekt musí souhlas udělit ke každému jednotlivému citlivému údaji zvlášť, resp. souhrnně, přičemž však každý citlivý údaj musí být vyjmenován. Není tak přípustné, aby byl souhlas udělen formou obecné formulace typu „Souhlasím se zpracováním svých osobních údajů.“[82]. Ostatně o vhodnosti použití této formulace lze pochybovat i v případě zpracování běžných osobních údajů, neboť jen stěží může splňovat povinnost správce informovat subjekt o rozsahu zpracovávaných osobních údajů nejpozději současně s udělením souhlasu[83].

Vzhledem k výše uvedené charakteristice souhlasu se nabízí otázka, zda může být souhlas se zpracováním ze strany subjektu odvolán. V původním znění zákona byla možnost odvolání souhlasu výslovně uvedena v § 5 odst. 5[84]. Rozsáhlou novelou Zákona č. 439/2004 Sb. však byl celý pátý odstavec zrušen. Podle důvodové zprávy k návrhu této novely vypuštěním tohoto odstavce nedošlo k oslabení postavení subjektu údajů, neboť otázka odvolatelnosti souhlasu úzce souvisí s požadavky na udělení souhlasu, na nějž se aplikují také obecné podmínky týkající se právních úkonů dle občanského zákoníku stanovící mimo jiné relativní

[81] Jak však uvádí ÚOOÚ ve svém rozhodnutí čj. SPR-5685/09, za konkludentní udělení souhlasu nemůže být považována pouhá nečinnost subjektu, pakliže subjekt o zpracování neví.
[82] Srov. též Stanovisko ÚOOÚ č. 2/2008 – Souhlas se zpracováním osobních údajů.
[83] Srov. Z rozhodovací činnosti ÚOOÚ – K souhlasu se zpracování osobních údajů (čj. 7/05/SŘ-OSČ).
[84] „..Souhlas je třeba dát v písemné formě a musí z něho být patrné, v jakém rozsahu je poskytován, komu a k jakému účelu, na jaké období a kdo jej poskytuje. Souhlas může být kdykoliv odvolán. ….“

neplatnost úkonu učiněného v omylu či tísni. Správce tak nemá povinnost informovat subjekt údajů o možnosti odvolání souhlasu; v případě, kdy však zpracované údaje získává přímo od subjektu, je povinen subjekt poučit o tom, zda je poskytnutí osobního údaje povinné či dobrovolné[85].

Pokud se týká výjimek ze zásady zpracování údajů výhradně se souhlasem subjektu, na prvním místě uvádí Zákon případ, kdy je zpracování nezbytné pro dodržení právních povinností správce (§ 5 odst. 2 písm. a) Zákona). Jestliže tedy správce není schopen splnit povinnost stanovenou mu konkrétním právním předpisem, aniž by zpracovával osobní údaje určitých subjektů, může tyto údaje zpracovávat i bez jejich souhlasu[86]. Zaměstnavatel tak nebude potřebovat souhlas svých zaměstnanců ke zpracování osobních údajů, bude-li je zpracovávat výhradně v rozsahu sloužícím splnění zákonem stanovených povinností (např. v oblasti sociálního zabezpečení).

Druhou z výjimek představuje situace, kdy je zpracování nezbytné pro plnění smlouvy nebo pro jednání o uzavření takové smlouvy, jejíž stranou je subjekt. Z mého pohledu je v těchto případech souhlas udělen konkludentně, a to právě poskytnutím údajů ze strany subjektu, který má zájem na plnění ze smlouvy a je si vědom toho, že bez zpracování poskytovaných osobních údajů se toto plnění stane nemožným (např. uvedení jména, bydliště a data narození pro účely nezaměnitelné identifikace smluvní strany)[87]. Na druhou stranu je evidentní, že správce nemůže tyto údaje využít za jiným účelem než plnění smlouvy (bez dalšího souhlasu) a přestane-li tento účel existovat, je správce povinen údaje zlikvidovat[88].

Další situace umožňující zpracovávat osobní údaje bez souhlasu subjektu jsou zejména případy, kdy

[85] Viz § 11 odst. 2 první věta ZOOÚ.
[86] Bartík, V., Janečková, E. *Zákon o ochraně osobních údajů s komentářem.* 1. vyd. Olomouc: ANAG, 2010, s. 87.
[87] Tamtéž.
[88] § 20 ZOOÚ

- je zpracování nezbytné k ochraně životně důležitých zájmů subjektu (§ 5 odst. 2 písm. c),
- se jedná o oprávněně zveřejněné osobní údaje (písm. d); v tomto případě je kladen důraz na slovo *oprávněně*, neboť o oprávněnosti zveřejnění značného množství údajů dostupných převážně z internetu by se dalo s úspěchem pochybovat. V případě zpracování takových údajů tak nemůže správce zákonnou výjimkou aplikovat a je povinen požádat subjekt o souhlas se zpracováním jeho údajů.
- je to nezbytné pro ochranu práv a právem chráněných zájmů správce (písm. e); v praxi bývá tohoto ustanovení využíváno zejména v případě zpracování osobních údajů pomocí kamerového systému se záznamem.
- se jedná o osobní údaje veřejně činné osoby, které vypovídají o veřejné činnosti (písm. f), nebo jde o zpracování výhradně pro účely archívnictví (písm. g).

4.2 Právo přístupu k informacím

V souladu s ustanovením § 12 Zákona je správce povinen poskytnout subjektu na jeho žádost informaci o zpracování jeho osobních údajů, a to bez zbytečného odkladu (žádost by však měla být podávána v rozumných intervalech; v extrémních případech – např. podávání žádosti každý den – by se ze strany subjektu mohlo jednat i o výkon práva v rozporu s dobrými mravy). Na rozdíl oproti informační a poučovací povinnosti správce dle § 11 Zákona, kterou vůči subjektu musí správce splnit již v okamžiku započetí se shromažďováním údajů (bez ohledu na to, zda je o to subjektem požádán), ustanovení § 12 umožňuje subjektu vyžádat si informace o zpracování svých údajů kdykoliv během celého procesu jejich zpracování. V tomto případě je to tedy subjekt, kdo musí vyvinout aktivitu a o poskytnutí informací správce sám požádat[89].

Správce je především povinen subjektu sdělit účel, rozsah a způsob zpracování, a také jej informovat o zdroji, z něhož osobní údaje získal (aby mohl

subjekt údajů posoudit, zda byly jeho údaje získány oprávněně, resp. také zda je jiný oprávněný správce nezákonně nezpřístupnil dalším osobám). Podle Zákona má být předmětem informace i sdělení o osobních údajích, případně kategoriích osobních údajů, které jsou předmětem zpracování. Je i v zájmu správce poskytnout subjektu informace o konkrétních údajích, které zpracovává, než odkaz na pouhou kategorii zpracovávaných údajů (např. „adresa“ namísto „Lhota 17, Lhota, PSČ 777 77“), protože teprve v návaznosti na poskytnutí konkrétních údajů může subjekt upozornit správce na jejich neaktuálnost či chybnost[90].

Správce je oprávněn požadovat za poskytnutí informací přiměřenou úhradu odpovídající jemu skutečně vzniklým nákladům (např. cena za pořízení kopií nebo poštovné). Pakliže správce zpracovává údaje prostřednictvím zpracovatele, je možné ve smlouvě o zpracování ve smyslu § 6 Zákona přenést informační povinnost na zpracovatele[91].

4.3 Právo obrátit se na kontrolní orgány

Právo obrátit se na Úřad pro ochranu osobních údajů poskytuje subjektu ustanovení § 21 odst. 3 a odst. 4 Zákona a souvisí s právem na řádné poučení subjektu ze strany správce (mimo jiné právě o právu obrátit se Úřad). Subjekt údajů by se měl s požadavkem na odstranění závadného stavu týkajícího se jeho osobních údajů obrátit nejprve na správce nebo zpracovatele a až poté, není-li náprava zjednána, kontaktovat Úřad; Zákon nicméně subjektu umožňuje správce či zpracovatele „přeskočit“ a obrátit se se svým podnětem na Úřad přímo. Subjekt by však tohoto oprávnění neměl zneužívat a zahlcovat Úřad svými podněty, a to zejména v případech, kdy se dá předpokládat spolupráce a snaha o nápravu ze strany správce[92]. Na Úřad by se tak měly obracet spíše subjekty těch údajů, jejichž údaje jsou zpracovávány zcela neoprávněně a komunikace mezi správcem a subjektem není možná. Jako sporná se však jeví otázka, zda je Úřad povinen se

[89] Srov. dokument sub. pozn. č. 86, s. 156.
[90] Srov. dokument sub. pozn. č. 86, s. 157.
[91] Tamtéž.
[92] Srov. dokument sub. pozn. č. 86, s. 190.

podněty dle § 21 odst. 3 a 4 Zákona zabývat. Souhlasím s výkladem potvrzeným a rozvinutým judikaturou Nejvyššího soudu[93], že v případě, kdy žádosti subjektu o nápravu správce či zpracovatel nevyhoví, a subjekt se v důsledku toho s touto žádostí obrátí na Úřad, je Úřad povinen se touto žádostí zabývat a věc prošetřit; v opačném případě by byl subjekt zbaven možnosti dosáhnout porušení ochrany svých osobních údajů. Obrátí-li se však subjekt na Úřad přímo, aniž by nápravu požadoval nejprve u správce, nemá na vyřízení takové žádosti ze strany Úřadu právní nárok[94].

Jak Úřad sám uvádí ve své Výroční zprávě za rok 2010, za posledních 5 let se počet stížností téměř ztrojnásobil. Nedůvodné stížnosti na porušování Zákona tak Úřad odkládá v souladu se správním řádem pouhým sdělením, že k porušení Zákona nedošlo a Úřad tak neshledal důvody k zahájení řízení z moci úřední. Stejně tak se Úřad nehodlá až na výjimky zabývat anonymními podáními, přičemž však bere v úvahu také důvodnou obavu stěžovatele z postihu ze strany správce údajů, což často bývá, jak ÚOOÚ uvádí, zřetelné zejména v oblasti pracovněprávních vztahů, a to včetně rizika ztráty zaměstnání či šikanózního postupu ze strany zaměstnavatele[95].

[93] Rozsudek Nejvyššího správního soudu sp.zn. 2 Ans 10/2008 ze dne 16.12.2008 a rozsudek Nejvyššího správního soudu sp.zn. 1 As 93/2009 ze dne 16.3.2010.
[94] Srov. dokument sub. pozn. č. 86, s. 190.
[95] Srov. Výroční zpráva ÚOOÚ za rok 2010, s. 39.

5. Povinnosti při zpracování osobních údajů

Jak již bylo výše uvedeno, způsobem, jímž právní úprava ochranu práv subjektů osobních údajů zajišťuje, je zejména stanovení minimálních požadavků zpracování pro osoby, které s těmito údaji nakládají či hodlají nakládat.

Účelem zákonného výčtu osob, jimž jsou stanoveny povinnosti při zpracovávání osobních údajů, je postihnout skutečně všechny osoby, které se na zpracování podílí. Zákon tak ukládá povinnosti nejen správci a zpracovateli, ale i jejich zaměstnancům a všem dalším osobám, které údaje zpracovávají na základě pověření či uzavřené smlouvy. Výčet těchto povinných osob nalezneme zejména v ustanovení § 13 – 15 Zákona, a to v souvislosti s požadavkem zabezpečení zpracovávaných osobních údajů.

Základní premisou ochrany osobních údajů je povinnost kohokoliv, kdo zpracovává osobní údaje subjektu, dbát při jejich zpracování na to, aby subjektu v důsledku zpracování nevznikla újma na právech (zejména právu na lidskou důstojnost) a také povinnost vyvarovat se neoprávněného zasahování (resp. jej nepřipustit) do soukromého a osobního života subjektu údajů, a to bez ohledu na to, z jakého titulu osobní údaje zpracovává[96]. Tato premisa je vyjádřena jak samostatně v ustanovení § 10 Zákona, na mnoha dalších místech Zákona – například hned v úvodním ustanovení, jakož i § 5 odst. 3 v rámci povinností správce[97]. Jedná se o požadavek ochrany základních práv upravených v čl. 10 Listiny základních práv a svobod, nicméně v ust. § 10 je zopakován proto, aby byl zřejmý jeho vztah ke zpracování osobních údajů, neboť právě při něm vzniká značné riziko porušování těchto základních práv[98].

[96] Srov. též Stanovisko ÚOOÚ č. 6/2009 – Ochrana soukromí při zpracování osobních údajů.
[97] Bartík, V., Janečková, E. *Zákon o ochraně osobních údajů s komentářem.* 1. vyd. Olomouc: ANAG, 2010, s. 148.
[98] Viz důvodová zpráva k zákonu č. 101/2000 Sb., sněmovní tisk č. 374/0, dostupná z http://www.psp.cz/sqw/text/tiskt.sqw?O=3&CT=374&CT1=0.

Při zpracování osobních údajů totiž k zásahu do soukromí nezbytně dochází (bez nakládání s projevy osobní povahy identifikované nebo identifikovatelné osoby by vlastně ke zpracování osobních údajů nikdy dojít nemohlo). Aby však byl tento zásah oprávněný, je nutné při zpracování dbát všech povinností stanovených Zákonem či popřípadě i dalšími právními předpisy. Zpracování údajů musí být zároveň prováděno způsobem a prostředky přiměřenými zvolenému (legálnímu) účelu zpracování[99].

Za účelem ochrany subjektů před neoprávněnými zásahy do soukromí proto Zákon stanoví zásady, které musí odpovědné osoby při zpracování údajů dodržovat a které jsou obsaženy především v ustanovení § 5 Zákona (na základě ustanovení § 7 se tyto povinnosti vztahují na zpracovatele stejně, resp. obdobně, jako na správce). Patřím sem zejména povinnost stanovit účel, způsob a prostředky zpracování, zpracovávat pouze přesné údaje a v případě potřeby je aktualizovat, shromažďovat údaje pouze v nezbytném rozsahu, údaje uchovávat pouze po nezbytnou dobu a v neposlední řadě také zpracovávat údaje pouze v souladu s účelem, k němuž byly shromážděny. Odpovědné osoby jsou také povinny zpracovávat osobní údaje pouze otevřeně, což však dle mého názoru v podstatě již vyplývá z ostatních povinností správce, má-li údaje zpracovávat v souladu se zákonem (zejména povinnost zpracovávat údaje s vědomím či přímo souhlasem subjektu a oznamovací povinnosti vůči ÚOOÚ), stejně tak zákaz shromažďovat údaje pod záminkou jiného účelu nebo činnosti (jedná se pouze o negativní vyjádření povinnosti stanovené v § 5 odst. 1 písm. f) Zákona) a údaje získané k různým účelům nesdružovat.

Následující subkapitoly se budou věnovat nejdůležitějším povinnostem osob zpracovávajících osobní údaje subjektů, o nichž dosud nebylo šířeji pojednáno v předchozí kapitole v souvislosti s korespondujícími právy subjektů údajů. Povinnost správce zpracovávat osobní údaje zásadně se souhlasem subjektu již

[99] Stanovisko ÚOOÚ č. 6/2009 – Ochrana soukromí při zpracování osobních údajů.

v této kapitole zmíněna nebude, neboť již byla rozebrána v souvislosti s odpovídajícím právem subjektu v předešlé kapitole.

5.1 Povinnost stanovit účel, prostředky a způsob zpracování

Ještě před zahájením zpracovávání osobních údajů je správce (pro zjednodušení bude dále z povinných osob zpracovávajících údaje uváděn pouze správce) povinen stanovit účel, k jehož dosažení mají být osobní údaje zpracovávány[100], tj. z jakého důvodu zamýšlí osobní údaje shromažďovat a dále s nimi nakládat. Podle recitalu 28 Směrnice musí být tento účel výslovný a legitimní a nelze jej po shromáždění údajů významně měnit. Sběr se navíc musí týkat pouze údajů, které jsou pro dosažení deklarovaného účelu podstatné, a jeho rozsah musí být přiměřený vzhledem ke všem okolnostem zamýšleného zpracování tak, aby nedocházelo k nadbytečnému zásahu do soukromí subjektu[101]. Poskytne-li tak kupříkladu zaměstnanec zaměstnavateli svou fotografii jako součást osobního spisu, není přípustné, aby tuto fotografii zaměstnavatel bez dalšího využil za jiným účelem (např. k otisknutí na vstupní kartu zaměstnance, byť obzvláště v takových případech zaměstnavatel souhlas se zpracováním fotografie často předpokládá, což ovšem rozhodně není správná praxe). Vymezení účelu musí[102] být dostatečně konkrétní a ověřitelné; nesmí se tedy jednat pouze o bezobsažnou deklaraci (např. „za účelem ekonomických zájmů zaměstnavatele“). V některých případech je účel stanovený přímo zákonem a správce jej tak sám formulovat nemusí (např. na úseku sociálního zabezpečení), v jiných jej vymezuje správce na základě svých vlastních soukromých zájmů. V každém případě však stanovený účel zpracování musí být jednoznačně seznatelný a ověřitelný a samozřejmě také pravdivý[103].

Stejně jako účel by i prostředky a způsob zpracování měly být stanoveny ještě před zahájením samotného zpracování. Není však vyloučeno, aby se na rozdíl

[100] § 5 odst. 1 písm. a) ZOOÚ
[101] Dokument sub. pozn. č. 96.
[102] Srov. též D´Ambrosová, H. *Ochrana osobních údajů při vedení personálních agend.* 1. vyd. Praha: Pragoeduca, 2002, s. 38.
[103] Srov. dokument sub. pozn. č. 97, s. 70.

od účelu v čase měnily, ukážou-li se jako nevyhovující či nevhodný. Prostředky, jimiž má být účelu zpracování údajů dosaženo, musí být přitom tomuto účelu přiměřené. Je-li tedy možné deklarovaného účelu dosáhnout i prostředky vůči soukromí jednotlivce méně invazivními, je zapotřebí využít právě těchto prostředků[104].

5.2 Povinnost při zabezpečení osobních údajů

Mezi významné povinnosti správce patří také povinnost zabezpečení osobních údajů[105], která by měla zabránit zneužití osobních údajů, k němuž by mohlo dojít nejen úmyslným jednáním správce, ale také v důsledku jeho nedbalosti. Dle čl. 17 Směrnice by měla být tato bezpečnostní opatření a náklady na jejich provedení přiměřená rizikům vyplývajícím ze zpracování daných údajů a povaze údajů, které mají být chráněny; rovněž i Zákon ponechává způsob a prostředky zabezpečení údajů na vlastní úvaze správce[106]. Údaje musí být chráněny zejména před náhodným nebo nedovoleným zničením, náhodnou ztrátou, neoprávněným přístupem a jakýmkoliv dalším neoprávněným zpracováním. Odpovědnost správce za bezpečnost chráněných údajů je přitom odpovědností objektivní, tj. odpovědností za následek bez ohledu na případné zavinění pachatele; dojde-li i přes bezpečnostní opatření k porušení ochrany osobních údajů, musí správce prokázat, že porušení nebylo možné ani při vynaložení veškeré péče zabránit (například že osobní spisy byly v sídle zaměstnavatele řádně uloženy a síla povodně, která je odnesla, se nedala předvídat)[107]. Na druhou stranu však lze za nedostatek právní úpravy považovat chybějící povinnost správce o případu neoprávněného zpracování či podobné události jako jsou ztráta, krádež, zpřístupnění třetím osobám apod. subjekt údajů neprodleně informovat, aby tento mohl na vzniklou situaci dle svého uvážení reagovat.

---

[104] Bartík, V., Janečková, E. *Ochrana osobních údajů v aplikační praxi.* 2. vyd. Praha: Linde, 2010, s. 62.
[105] § 13 ZOOÚ
[106] Rozsudek NSS sp.zn. 3 As 21/2005 ze dne 10.5.2006.
[107] Srov. též Z rozhodovací činnosti ÚOOÚ – Povinnost zabezpečit osobní údaje, zproštění odpovědnosti (čj. VER-6243/08-17). Liberační důvod je uveden v ust. § 46 odst. 1 ZOOÚ.

Bezpečnostní opatření přijatá za účelem ochrany zpracovávaných osobních údajů budou samozřejmě u každého správce různá, a to vzhledem k odlišnosti podmínek u jednotlivých správců. Rozhodující pro správce však bude dodržení minimální ochrany, která je pro danou technologii považována za standard[108]. Vodítka k přijetí opatření obsahuje ust. § 13 Zákona v odst. 3 vyjmenováním rizik, jež mají být při přijímání opatření posouzena; pro automatizované zpracování navíc přidává správci či zpracovateli další povinnosti v odst. 4. Bezpečnostní opatření přitom mohou být různé povahy: od fyzického zajištění bezpečnosti jako jsou zámky, alarmy, mříže, přes kontroly vstupu osob až po zabezpečení technologická. Jedno ze základních opatření je však určení podmínek, které jsou jednotliví zaměstnanci nebo jiné osoby přicházející do styku s osobními údaji povinni dodržovat[109]. Tyto podmínky by se měly týkat jak osobních údajů ve fyzické podobě (např. uzamykání skříně s osobními spisy), tak v podobě elektronické (zákaz kopírování údajů na přenosná záznamová zařízení, zákaz sdělování přístupového hesla třetím osobám, a to i v době nepřítomnosti zaměstnance apod.). Velice účelný je také systém ověřující, zda osoba přistupující k údajům má k tomu přístupu oprávnění, jakož i registrace a uchovávání zaznamenaných přístupů k údajům – tento postup lze aplikovat jak na data fyzická (vstupní karta do místnosti s osobními spisy) tak data elektronická (login každého jednotlivce, heslo).

V souladu se čl. 17 a 18 Směrnice stanoví Zákon v § 13 povinnost správce vypracovat a dokumentovat přijatá a provedená bezpečnostní opatření. Zákon však nestanoví, že by tato opatření musela být obsažena v jednom dokumentu ani to, jakou má mít tento dokument formu či obsah (např. „směrnice zaměstnavatele o ochraně osobních údajů“). Přestože je shromáždění pravidel týkající se nakládání a zajištění bezpečnosti zpracovávaných osobních údajů v jednom dokumentu jistě vhodnější, v úvahu připadá i jejich rozdělení do jednotlivých interních předpisů

[108] Srov. rozsudek NSS sp.zn. 3 As 21/2005 ze dne 10.5.2006.
[109] Viz Z rozhodovací činnosti ÚOOÚ – K povinnosti správce osobních údajů podle § 13 zákona č. 101/2001 Sb. (čj. 2/05/SŘ-OSČ).

zaměstnavatele (resp. správce)[110]. Obzvláště zpracování osobních údajů ve větším rozsahu nebo zpracování citlivých údajů však vyžaduje od zaměstnavatele také zajištění pravidelného proškolování zaměstnanců o obsahu předpisu[111], jakož i přiměřenou kontrolo jeho dodržování[112]. Opět je totiž na správci, aby v případě vzniku pochybností prokázal existenci výše uvedených stejně jako skutečnost, že s nimi byly osoby přicházející do styku s osobními údaji seznámeny a že jejich dodržování bylo ze strany správce důsledně vyžadováno. Selhání jednotlivých zaměstnanců při jinak adekvátních bezpečnostních opatřeních by totiž mohlo představovat liberační důvod správce pro zproštění se odpovědnosti dle ustanovení § 46 odst. 1 Zákona[113].

Pakliže však správce přijetí takových pravidel nebude schopen prokázat, budou se veškeré běžné postupy zaměstnanců při nakládání s osobními údaji považovat za postupy správcem schválené a za případné porušení právních předpisů při zpracování těchto údajů bude odpovědný právě správce, byť by k porušení došlo prostřednictvím jeho zaměstnance či jiné pověřené osoby[114] (s výjimkou uplatnění liberačního důvodu, jak bylo vysvětleno výše). K naplnění skutkové podstaty správního deliktu podle § 45 odst. 1 písm. h) Zákona (tj. porušení povinnost řádného zabezpečení údajů) navíc postačí i stav, kdy k neoprávněnému zpracování dojít může, tj. pouhé ohrožení zpracovávaných údajů. Neoprávněné zpřístupnění údajů třetí osobě či jejich zneužití jsou pak již pouze následkem absence či nízké kvality bezpečnostních opatření[115].

K ochraně údajů přitom může přispět i zdánlivá maličkost – například umístění zálohovacích médií v bezpečné zóně, aby se zabránilo jejich případnému zničení v případě havárie v hlavních prostorách, a samozřejmě umožnění přístupu

[110] Srov. dokument sub. pozn. č. 97, s. 163.
[111] Jak uvádí WP 29 ve svém stanovisku WP 48 o zpracování osobních údajů v souvislosti se zaměstnáváním, adekvátní míry ochrany soukromí zaměstnanců na pracovišti nemůže být dosaženo bez odpovídajícího vyškolení osob, která s osobními údaji zaměstnanců nakládají.
[112] Z rozhodovací práce ÚOOÚ – K zabezpečení osobních údajů zpracovávaných výpočetní technikou, čj. SPR-356/07.
[113] Srov. dokument sub. pozn. č. 97, s. 167.
[114] Dokument sub. pozn. č. 104, s. 92.
[115] Viz dokument sub. pozn. č. 109.

k osobním údajům pouze těm zaměstnancům či osobám, které přístup skutečně potřebují (princip „need to know“)[116].

5.3 Povinnost informovat subjekt údajů o zpracovávání

Informační povinnost správce je další ze základních zásad ochrany osobních údajů, neboť pouze tehdy, je-li subjekt údajů informován o tom, že jsou jeho údaje zpracovávány a v jakém rozsahu k tomu dochází, se může sám aktivně podílet na jejich ochraně a kontrole tohoto zpracovávání[117]; v případě zjištění neoprávněného zásahu má poté možnost domáhat se ochrany ze strany státních orgánů (především ÚOOÚ). Pokud by však subjekt o zpracování nevěděl, nemohl by nakládání se svými osobními údaji nikterak ovlivnit. Přestože nelze předpokládat, že by většina osob, jejichž údaje jsou zpracovávány, po poskytnutí těchto údajů nadále jevila zájem o informace, jak je s nimi nakládáno, toto právo jim jako subjektu údajů nemůže být upřeno. Informační povinnost podle § 11 Zákona se tak vztahuje nejen na zpracovávání osobních údajů na základě souhlasu subjektu, ale také na zpracovávání údajů na základě zákona, kdy správce není povinen si souhlas subjektu vyžádat. I v tomto případě však musí být subjekt údajů o zpracování i jeho charakteru dostatečně informován. Pokud navíc správce získává osobní údaje přímo od subjektu, je povinen jej poučit o tom, zda je jejich poskytnutí dobrovolné či nikoli; v případě, kdy je subjekt povinen správci údaje poskytnout, musí být poučen o důsledcích v případě, že tak odmítne učinit.

V praxi je nejčastěji informační povinnost správce plněna prostřednictvím textu, který je zapracován do dokumentu souhlasu[118] (obvykle označeném jako „Souhlas se zpracováním osobních údajů“). Přestože Zákon nestanoví, že by informační povinnost musela být splněna písemně, nelze správcům jiný způsob informování subjektu doporučit (či si poskytnutí informací nechat alespoň písemně

[116] Srov. Z rozhodovací činnosti ÚOOÚ – K zabezpečení osobních údajů (čj. VER -3280/08-34).
[117] Bartík, V., Janečková, E. Jak plnit informační povinnost podle zákona o ochraně osobních údajů. *Právní rádce.* 2011, č. 5, s. 32.
[118] Z rozhodovací činnosti ÚOOÚ – K plnění informační povinnosti (čj. 26/05/SŘ-OSČ, 50/05/SŘ-OSČ, 70/05/SŘ-OSČ).

ze strany subjektu potvrdit[119]). Ačkoliv u informační povinnosti správce není podobné ustanovení jako u souhlasu subjektu, podle kterého musí být poskytnutí souhlasu správce schopen kdykoliv během zpracovávání prokázat, za použití analogie by se důkazní břemeno na straně správce dalo dle mého názoru dovodit i u informační povinnosti. Se zřetelem na tuto skutečnost je proto potřeba přistupovat i k výjimkám zprošťujícím správce informační povinnosti uvedeným v ustanovení § 11 odst. 3 ZOOÚ (případy, kdy údaje správce nezískal přímo od subjektu údajů), neboť případné nesplnění poučovací povinnosti je spojeno se sankcemi ze strany Úřadu[120]. Správce je sice oprávněn splnit svou informační povinnost také prostřednictvím zpracovatele (§ 11 odst. 7 Zákona), toto přenesení však správce odpovědnosti za splnění povinnosti nezbavuje.

Správce je především povinen informovat subjekt o tom, v jakém rozsahu, za jakým účelem, jakým způsobem a kým budou osobní údaje subjektu zpracovávány a komu mohou být dále zpřístupněny, přičemž tyto osoby musí být dostatečně identifikovány[121]. Tím však rozsah informační povinnosti zdaleka nekončí. Správce je dále povinen poučit subjekt o jeho právu přístupu k údajům a také o tom, zda je poskytnutí těchto údajů dobrovolné či povinné, popř. jaké důsledky by odmítnutí poskytnutí údajů mohlo pro subjekt mít. Subjekt musí být také poučen o svém právu domáhat se nápravy v případě, že zpracování nebude probíhat v souladu se zákonem, a také o možnosti obrátit se přímo na Úřad[122] (v této souvislosti bývá správcům doporučováno uvést v poučení i kontaktní informace Úřadu; dle mého názoru však toto není absolutně nezbytné a na absenci této informace by nemělo být nahlíženo jako na nesplnění zákonných povinností). Poučení musí rovněž zahrnovat informaci o tom, že v případě porušení povinností při zpracování odpovídají správce a zpracovatel společně a nerozdílně a že v případnou nemajetkovou újmu může subjekt uplatňovat v souladu s občanským

[119] Srov. dokument sub. pozn. č. 117, s. 35.
[120] § 44 odst. 2 písm. f), resp. § 45 písm. f) ZOOÚ
[121] Nedostačujícím je např. označení „obchodní společnosti na území České republiky“ – viz dokument sub. pozn. č. 118.
[122] § 21 odst. 1, 3 a 4 ZOOÚ

zákoníkem[123] (subjekt se tedy může domáhat, zejména aby bylo upuštěno od neoprávněných zásahů do jeho práva na ochranu osobnosti, aby byly odstraněny následky těchto zásahů a aby mu bylo dáno přiměřené zadostiučinění; v případě výrazného zásahu do lidské důstojnosti či pověsti má právo domáhat se také náhrady nemajetkové újmy v penězích).

5.4 Oznamovací povinnost

Písemnou oznamovací povinnost vůči ÚOOÚ má obecně podle § 16 Zákona každý, kdo hodlá jako správce zpracovávat osobní údaje anebo je zpracovávat nadále jinak, než jak bylo uvedeno v jeho předchozím oznámení. Vzhledem k použití slova „hodlá" je jednoznačné, že oznámení musí být správcem učiněno ještě před započetím zpracovávání[124]. Pro úplnost je nutné rovněž doplnit, že na rozdíl od některých dalších povinností se oznamovací povinnost vztahuje výlučně na správce a nikoliv zpracovatele, resp. další osoby. Je to totiž právě správce, kdo určuje účel a prostředky zpracování osobních údajů a kdo případně pověřuje další osoby k jejich zpracování. [125] Oznamovací povinnost se přitom vztahuje na všechny správce, kteří osobní údaje zpracovávají na území České republiky – tedy také na správce se sídlem mimo území České republiky, kteří zde údaje zpracovávají prostřednictvím třetích osob.[126]

Ne všichni správci však musí plánované zpracování osobních údajů oznamovat. Pro správné určení, zda se na danou osobu vztahuje oznamovací povinnost ve smyslu § 16, je nejprve nezbytné určit:

- zda se jedná o správce osobních údajů,
- zda se jedná o zpracovávání údajů ve smyslu ZOOÚ, a

[123] § 21 odst. 5 a 6 ZOOÚ
[124] Morávek, J. *Ochrana osobních údajů v pracovněprávní agendě.* 1. vyd. Praha: BMSS Start, 2010, s. 64.
[125] Srov. dokument sub. pozn. č. 97, s. 170-171.
[126] Viz též www.uoou.cz / Názory Úřadu / Často kladené otázky. Jedním z případu může být zpracování údajů v rámci koncernu, kde správcem (a tedy subjektem, který určuje účel a prostředky zpracování) je zahraniční mateřská společnost, která zpracování provádí

- zda se na danou situaci a správce nevztahuje některý z případů uvedený v ustanovení § 18 ZOOÚ.

Jestliže na základě vyhodnocení výše uvedených kritérií bude konkrétní správce oznamovací povinnosti podléhat, musí jeho oznámení vůči Úřadu obsahovat informace uvedené v ustanovení § 16 odst. 2 Zákona. Jelikož se toto oznámení podává Úřadu na registračním formuláři v elektronické podobě, je celý postup značně zjednodušen (po správci je vyžadováno zejména uvedení rozsahu zpracovávaných údajů, způsobu, prostředků a místa zpracování, označení příjemců údajů či přijatá bezpečnostní opatření). Podání oznámení není nijak zpoplatněno (oproti kupříkladu návrhu na zápis či změnu v obchodním rejstříku), na základě plné moci jej navíc za správce může podat i další osoba (obecný zmocněnec, advokát apod.) Na základě svého oznámení je správce oprávněn zahájit zpracovávání dnem svého zápisu do registru vedeném Úřadem podle § 35 Zákona a zveřejněném na webových stránkách Úřadu nebo po uplynutí lhůty 30 dnů ode dne doručení oznámení Úřadu[127]. Není tedy nutné, aby správce vyčkával celých třicet dní, než s plánovaným zpracováním započne; objeví-li se jeho oznámené zpracovávání v registru i před uplynutím této lhůty, může začít se zpracováváním ihned. Osvědčení o registraci se pak vydává pouze na žádost oznamovatele[128]. V případě, že správce podléhající oznamovací povinnosti hodlá ukončit svou činnost, je podle § 19 Zákona povinen Úřadu neprodleně oznámit, jak s osobními údaji po ukončení své činnosti naloží.

Výjimky z oznamovací povinnosti správců upravuje § 18 Zákona. Oznamovací povinnost se tak nevztahuje na zpracování osobních údajů, které správce získal z veřejně dostupných zdrojů nebo mu jejich zpracování ukládá zvláštní zákon nebo pokud se jedná o zpracování v rámci oprávněné činnosti sdružení a pro jeho vnitřní potřebu.

---

prostřednictvím svých dceřiných společností se sídlem v jednotlivých zemích (včetně ČR), v nichž jí také (v závislosti na vnitrostátní úpravě) vzniká oznamovací povinnost.

[127] § 16 odst. odst. 3 ZOOÚ

[128] § 16 odst. 5 ZOOÚ

V prvním z uvedených případů hovoří zákon o zpracování osobních údajů, které jsou součástí veřejně přístupných datových souborů. Za takový soubor dat (v podstatě jakousi databázi) se považuje například obchodní rejstřík, katastr nemovitostí a další registry a údaje v nich obsažené, které jsou na základě příslušných zákonů zpřístupněny veřejnosti. Oznamovací povinnost je zde vtažena do souvislosti s oprávněním správce zpracovávat údaje bez souhlasu subjektu tehdy, jedná-li se o oprávněně zveřejněné osobní údaje ve smyslu § 5 odst. 2 písm. b) Zákona. Zákon zde zdůrazňuje oprávněnost takového zveřejnění, neboť bohužel nikoliv všechny veřejně přístupné údaje byly zveřejněny v souladu s právními předpisy (tzn. nejen Zákonem, ale i občanskoprávními a dalšími předpisy), a to zejména jedná-li se o zveřejnění prostřednictvím médií (srov. též část v předchozí kapitole věnující se nutnosti udělení souhlasu ze strany subjektu zpracovávaných osobních údajů)[129].

Velice důležitým důvodem osvobozujícím mnoho správců z oznamovací povinnost je pak případ druhý, tj. jestliže je zpracování údajů správci uloženo zákonem[130]. I zde Zákon nepřímo odkazuje na souvislost s absencí souhlasu subjektu ke zpracování, a to v případě, je-li zpracování nezbytné pro dodržení právní povinnosti správce v souladu s ustanovením § 5 odst. 2 písm. a) Zákona. Obzvláště zaměstnavatelé na tuto výjimku často zapomínají, a zpracování osobních údajů zaměstnanců, které jim ukládají zvláštní předpisy (např. v oblasti sociálního zabezpečení či zdravotního pojištění, v oblasti daňové či mzdové), Úřadu oznamují, byť oznamovací povinnosti podle § 16 nepodléhají – právě zpracování osobních údajů zaměstnanců je totiž nezbytné pro dodržení zaměstnavatelových právních povinností uložených mu zvláštními zákony[131]. Na druhou stranu je však zapotřebí zdůraznit, že oznamovací povinnosti jsou zaměstnavatelé (resp. všichni správci) zproštěni jen v rozsahu, v jakém jim zvláštní předpis zpracování ukládá. Získává-li tedy zaměstnavatel od svých zaměstnanců i jiné osobní údaje nebo již

[129] Srov. dokument sub. pozn. č. 97, s. 179.
[130] § 18 odst. 1 písm. b) ZOOÚ
[131] Viz také ÚOOÚ k problémům z praxe č. 2/2005 – Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů.

zpracovávané osobní údaje hodlá využít pro své vlastní soukromé účely, oznamovací povinnosti v rozsahu těchto „nadstandardně“ požadovaných osobních údajů podléhat bude. I správce nepodléhající oznamovací povinnosti podle § 18 odst. 1 písm. b) Zákona však musí informace, které by jinak byly předmětem oznámení vůči Úřadu, zpřístupnit, a to jakoukoliv vhodnou formou – nejčastěji prostřednictvím internetu nebo jiným způsobem umožňujícím dálkový přístup[132].

I na tomto místě dále považuji za významné opakovaně zdůraznit, že i při osvobození správce od oznamovací povinnosti je správce povinen při zpracování osobních údajů dbát na ochranu soukromého a osobního života subjektu ve smyslu § 5 odst. 3 a § 10 Zákona.

5.5 Povinnost zpracovatele

V ustanovení § 8 Zákona nalezneme povinnost určenou výhradně zpracovateli nad rámec ostatních povinností společných všem osobám zpracovávajícím osobní údaje. Podle tohoto ustanovení je zpracovatel povinen upozornit správce, zjistí-li, že porušuje své zákonné povinnosti, a ukončit zpracování osobních údajů. Jestliže tak zpracovatel neučiní, odpovídá společně a nerozdílně za škodu, která případně subjektu vznikne; ustanovení § 8 tedy obsahuje liberační důvod ze solidární odpovědnosti správce a zpracovatele podle § 21 odst. 6 ZOOÚ.

Jak uvádí poslední věta § 8, není touto možností liberace dotčena odpovědnost zpracovatele za plnění povinností ZOOÚ, které musí plnit každý subjekt zpracovávající osobní údaje. Není tedy možné neplnit například povinnost řádného zabezpečení osobních údajů s odkazem na skutečnost, že o tomto nedostatku zpracovatel správce informoval[133].

[132] § 18 odst. 2 ZOOÚ
[133] Srov. dokument sub. pozn. č. 97, s. 115.

6. Osobní údaje v pracovněprávních vztazích

Po vysvětlení terminologie používané v oblasti ochrany osobních údajů a pojednání o jednotlivých právech subjektů údajů a povinnostech osob, které údaje zpracovávají, bych se v této části práce ráda zaměřila na specifika zpracovávání osobních údajů v pracovněprávních vztazích. I přes poměrně velký počet publikací v této oblasti vyvstávají při každodenní činnosti zaměstnavatelů (resp. jejich zaměstnanců působících v personálním oddělení) nové a nové otázky ohledně nakládání s osobními údaji zaměstnanců a vysoké procento zaměstnavatelů nemá v této oblasti zcela jasno, což bohužel souvisí i s chápáním problematiky ochrany osobních údajů jako oblasti okrajové a pro podnikatelskou činnost nedůležité.

Osobní údaje zaměstnanců i uchazečů o zaměstnání jsou přitom pro zaměstnavatele absolutně nezbytné, neboť právě jejich znalost jim umožňuje vhodně využít zaměstnancův potenciál či vybrat uchazeče, který bude nejlépe odpovídat profilu daného pracovního místa. Tendencí zaměstnavatelů však bývá zjišťovat o svých zaměstnancích naprosté maximum informací, a to i takových, které s pracovněprávním vztahem absolutně nesouvisí. Zaměstnavatelé mívají často pocit, že čím více údajů budou o svých zaměstnancích znát, tím vyšší pracovní efektivity jim to umožní dosáhnout. I v souvislosti s tím je třeba stanovit, které osobní údaje musí zaměstnavatel u svých zaměstnanců znát, které od nich požadovat může, a také vymezit, které osobní údaje zaměstnavatel od zaměstnance vyžadovat nesmí. Za každých okolností však platí, že zaměstnavatel musí ke všem osobním údajům získaným v souvislosti s pracovněprávními vztahy přistupovat nikoli jako k vlastnictví jeho samotného, nýbrž vlastnictví svých zaměstnanců či uchazečů o pracovní pozici, kteří mu je pouze propůjčili k určitým, předem vymezeným účelům[134].

[134] www.uoou.cz / Dozorová činnost / Kontrolní činnost inspektorů / Kontroly v minulosti – 2007 / Zaměstnavatel jako správce osobních údajů

Jak již bylo řečeno v předchozích kapitolách, právo na ochranu osobních údajů představuje nedílnou část jednoho ze základních práv každého jedince, a to práva na ochranu soukromí a osobního života. Ve vztahu k soukromí na pracovišti je v odborné literatuře často zmiňováno rozhodnutí Evropského soudu pro lidská práva ve věci Niemietz proti Německu ze dne 12.12.1992, podle něhož je pod pojmem soukromí člověka nutné rozumět právo člověka na zakládání a rozvíjení vztahů s ostatními lidmi, a to i v rámci profesního života, neboť právě po dobu pracovních aktivit má většina lidí největší příležitost k navazování kontaktů s vnějším světem. Je proto nesporné, že zaměstnavatel je povinen respektovat soukromí svých zaměstnanců i během jejich pracovní doby, resp. jejich pobytu na pracovišti[135], a to i vzhledem ke skutečnosti, že často není možné zřetelně rozlišit, které z aktivit zaměstnance striktně souvisí s výkonem jeho pracovní činnosti a které jsou naopak čistě soukromé povahy. Přestože, jak bude později vysvětleno, je možné toto právo na soukromí na pracovišti do jisté míry omezit, má-li k tomu zaměstnavatel legitimní důvod; nikdy však nesmí být omezeno více, než je v daném případě nezbytně nutné.

Zaměstnavatel proto vždy musí v souladu s ustanovením § 10 Zákona respektovat zásadu proporcionality a o svých zaměstnancích shromažďovat pouze takové údaje, které potřebuje ke své činnosti; nesmí tedy zasahovat do jejich soukromí v míře větší, než je nezbytně nutné. Rozsah zjišťovaných údajů se samozřejmě bude lišit v závislosti na charakteru činnosti zaměstnavatele (rozsah požadovaných informací může být širší, přichází-li například zaměstnanec do styku s dětmi či nakládá s cennými věcmi), v žádném případě však není zaměstnavatel oprávněn zjišťovat informace či požadovat předložení listin, které s pracovněprávním vztahem nijak nesouvisejí (např. požadovat předložení rozsudku o vypořádání společného jmění manželů).

[135] Srov. též Morávek, J. *Ochrana osobních údajů v pracovněprávní agendě.* 1. vyd. Praha: BMSS Start, 2010, s. 12.

Při získávání a shromažďování osobních údajů zaměstnanců se zaměstnavatel dostává do pozice správce, a jako takový musí samozřejmě dodržovat povinnosti správce stanovené Zákonem, z nichž ty nejdůležitější byly rozebrány v předchozí kapitole. Zaměstnavatelé rovněž často opomíjejí řádné zabezpečení osobních údajů svých zaměstnanců, které má zabránit neoprávněnému či nahodilému přístupu třetích osob k těmto údajům nebo jejich zneužití (např. situace, kdy personalistka ukládá osobní spisy zaměstnanců pouze do skříně, aniž by ji při svém odchodu uzamkla, či jejich obsah zpřístupňuje i osobám, které k tomu nejsou oprávněné). Typickým příkladem také bývá zpřístupnění osobních údajů o uchazečích širokému okruhu stávajících zaměstnanců, aniž by to bylo odůvodněné. Nedostatky bývají i v zabezpečení údajů uložených na datových nosičích, např. firemním serveru. Samozřejmostí by mělo být omezení přístupu oprávněným osobám výhradně za použití loginu/čipu/jiného identifikátoru a hesla tak, aby bylo možné zpětně dohledat, kdo a kdy s údaji nakládal[136]. Rovněž je nutné chránit datové úložiště proti útokům zvenčí. Více k problematice zabezpečení údajů však bylo uvedeno již v subkapitole 5.2, a proto ji zde již nebudu dále rozvádět.

6.1 Osobní údaje zpracovávané před uzavřením pracovního poměru

Právní úprava práv a povinností subjektů v tzv. prepracovních vztazích, to jest před vznikem samotného pracovněprávního vztahu, je do jisté míry kusá a v zásadě se omezuje pouze na zajištění rovného zacházení se všemi účastníky[137], a to v souvislosti s vývojem legislativy v rámci opatření proti diskriminaci dokonce hned několikrát (zákoník práce, zákon o zaměstnanosti, antidiskriminační zákon). Při výběru zaměstnance se proto zaměstnavatel musí vypořádat se dvěmi protichůdnými zásadami: jednak zásadou smluvní volnosti a svobodného rozhodování o výběru smluvního partnera na straně jedné a jednak zásadou zákazu

[136] Obvykle s využitím tzv. logových souborů zaznamenávajících údaje o veškeré aktivitě uživatelů, kteří se do systému přihlásili.
[137] Matoušová, M. a kol. *Ochrana osobních údajů v otázkách a odpovědích*. 1. vyd. Praha: ASPI Publishing, 2004, s. 49.

diskriminace, tj. zákazem požadování a vyhodnocování takových informací, které přímo nesouvisejí s pracovním uplatněním uchazeče, na straně druhé[138].

Ve vztahu k jednání před vznikem pracovního poměru zákoník práce v ustanovení § 30 odst. 2 stanoví, že zaměstnavatel smí vyžadovat od uchazeče o práci pouze takové údaje, které bezprostředně souvisí s uzavřením pracovní smlouvy (analogicky můžeme toto ustanovení vztáhnout i na dohody o práci konané mimo pracovní poměr). V souvislosti s tím není zaměstnavatel oprávněn zjišťovat od uchazeče údaje, jejichž znalost by mohla vést k uchazečově diskriminaci při výběru zaměstnance[139] a není také oprávněn požadovat informace v rozsahu, jenž je nezbytný až v případě, bude-li s uchazečem pracovní poměr či jiný pracovně právní vztah skutečně uzavírán (např. počet dětí)[140]. Ustanovení § 12 odst. 2 ZZ pak zakazuje zaměstnavateli vyžadovat při výběru svých zaměstnanců některé z citlivých údajů[141] a také ty informace, které odporují dobrým mravům. Jako poslední musí zaměstnavatel zohlednit ustanovení § 316 odst. 4 ZP, které sice týká vyžadování informací od zaměstnanců (tj. nikoli „pouhých" uchazečů o zaměstnání), nicméně výkladem a minori ad maius je třeba dojít k závěru, že se toto ustanovení bude vztahovat i na uchazeče[142]. Informace uvedené v tomto ustanovení zaměstnavatel nesmí získávat ani prostřednictvím dalších osob.

Z citlivých údajů je tak zaměstnavatel oprávněn požadovat pouze údaje o odsouzení za trestný čin či údaje o zdravotním stavu (včetně případného těhotenství), pakliže je pro to dán věcný důvod spočívající v povaze práce, která má být vykonávána, a je-li tento požadavek přiměřený (§ 316 odst. 4 ZP); na žádost uchazeče je však zaměstnavatel povinen prokázat uchazeči potřebnost požadovaného osobního údaje (§ 12 odst. 2 ZZ). V reálném životě však odstranění jakékoliv diskriminace v přístupu k zaměstnání bude jen obtížně uskutečnitelné,

[138] Mališ, P. Ochrana osobních údajů na pracovišti a povinnosti zaměstnavatelů. *Personální a sociálně právní kartotéka.* 2009, č. 12, s. 3.
[139] Srov. § 4 a 12 zákona o zaměstnanosti, § 5 antidiskriminačního zákona, § 16 ZP.
[140] Jouza, L. Ochrana osobních práv zaměstnance. *Bulletin advokacie.* 2008, č. 6, s. 35.
[141] Tento zákaz je však prolomen v případech dle § 4 odst. 3 a 4 ZZ.
[142] Bělina, M. a kol. *Zákoník práce. Komentář.* 2. vyd. Praha: C.H. Beck, 2010, s. 134.

neboť i pouhým setkáním s uchazečem bez poskytnutí jakýchkoliv informací zaměstnavatel zjistí minimálně přibližný věk, pohlaví a rasu uchazeče, přičemž už samotná znalost těchto údajů může vést ke znevýhodnění daného kandidáta (možné mateřství, důchodový věk atd.).

Ne všechny osobní údaje se však k zaměstnavatelům dostanou proto, že by je sami vyžadovali. V případě zveřejnění inzerátu s nabídkou zaměstnání, vypsání výběrového řízení a často dokonce i bez jakéhokoliv vyžádání dostává zaměstnavatel od uchazečů o zaměstnání životopisy, motivační dopisy, jakož i další dokumenty obsahující osobní údaje uchazečů. Jak již bylo uvedeno v subkapitole 4.1, souhlas ze strany uchazeče ke zpracování osobních údajů je de facto zaměstnavateli poskytnut již tím, že mu dané údaje zpřístupní, a tudíž musí být evidentně informován o tom, komu a které své osobní údaje poskytuje a rovněž pro jaký účel tak činí. V úvahu také připadá aplikace ust. § 5 odst. 2 písm. b) Zákona, podle něhož je správce oprávněn zpracovávat osobní údaje tehdy, je-li to nezbytné pro jednání o uzavření smlouvy uskutečněné na návrh subjektu údajů[143]. Zaměstnavatel v roli správce je však povinen použít údaje výhradně pro daný účel (tedy jednání o uzavření pracovněprávního vztahu) a uchovávat je pouze po dobu nezbytně nutnou[144]. Po skončení výběrového řízení je proto povinen osobní údaje neúspěšnému uchazeči vrátit či je řádně zlikvidovat[145]. Bude-li si chtít údaje uchazeče uchovat i posléze, např. pro výběrová řízení v budoucnosti, je oprávněn tak učinit pouze se souhlasem uchazeče; neúspěšný uchazeč totiž může oprávněně předpokládat, že jednání o uzavření smlouvy bylo výběrem jiného uchazeče ukončeno[146].

Ke zjišťování osobních údajů o uchazečích, jakož i o zaměstnancích obvykle zaměstnavatelé využívají různé formy osobního dotazníku. V případě uchazečů by takový dotazník měl obsahovat informaci o tom, že sdělované osobní údaje jsou

[143] Výroční zpráva ÚOOÚ za rok 2008, s. 69.
[144] § 5 odst. 1 písm. d) a e) ZOOÚ
[145] Bartík, V., Janečková, E. Zpracování osobních údajů před uzavřením pracovního poměru. *Personální a sociálně právní kartotéka.* 2010, č. 11, s. 4.

potenciálnímu zaměstnavateli poskytovány pro účely výběrového řízení[147], v případě stávajících zaměstnanců by poskytnutí údajů mělo být omezeno na dobu trvání pracovního poměru s maximálním omezením této doby. Je nepřípustné, aby byl souhlas udělován bez časového omezení (de facto na celý život), a to i za předpokladu, že subjekt údajů má právo svůj souhlas kdykoliv odvolat. Jestliže se zaměstnavatel rozhodne přistoupit k vytvoření databáze potenciálních kandidátů na budoucí volná pracovní místa, i zde je nezbytné uchovávat tyto údaje pouze po nezbytně nutnou dobu. Jelikož je zaměstnavatel povinen dodržovat Zákonem stanovenou povinnost zpracovávat pouze přesné a aktuální údaje, je otázka, jaká doba bude pro uchování údajů o uchazeči považována za přiměřenou. I toto bude souviset s konkrétními okolnostmi a potřebami zaměstnavatele, domnívám se však, že je nepřípustné, aby byly osobní údaje uchazečů bez jejich aktualizace uchovávány déle než jeden rok[148]. Ohledně vedení databáze uchazečů bude mít navíc zaměstnavatel oznamovací povinnost v souladu s ustanovením § 16 Zákona, neboť v takovém případě nelze aplikovat žádnou zákonnou výjimkou z této povinnosti.

S ohledem na zásady uvedené výše je tak zaměstnavatel oprávněn požadovat před vznikem pracovněprávního vztahu zejména následující údaje (v závislosti na charakteru pracovní pozice může zaměstnavatel samozřejmě požadovat i další informace)[149]:

– *jméno, příjmení, titul, rodné a všechna předcházející příjmení*[150]

Tyto údaje jsou k uzavření smluvního vztahu absolutně nezbytné, neboť bez nich není možné druhou kontraktační stranu řádně identifikovat.

---

[146] Z rozhodovací činnosti ÚOOÚ – Ke zpracování osobních údajů uchazečů o zaměstnání (čj. SKO-0629/07).
[147] V této souvislosti lze uvažovat o možné době uchování těchto údajů až po dobu tří let, a to jako důkazních prostředků pro možný spor o to, zda zaměstnavatel nepostupoval při výběru zaměstnanců diskriminačně. Srov. též dokument sub. pozn. č. 135, s. 73.
[148] Autoři Bartík a Janečková ve svém článku (dokument sub. pozn. č. 145) uvádí jako přiměřenou dobu šesti měsíců.
[149] Dokument sub. pozn. č. 145, s. 3.
[150] D´Ambrosová, H. *Ochrana osobních údajů při vedení personálních agend.* 1. vyd. Praha: Pragoeduca, 2002, s. 22.

– *datum narození*

Tento údaj také slouží k identifikaci zaměstnance.

– *adresa bydliště a další obvyklé kontaktní údaje*[151]

Jedním z kontaktních údajů zaměstnance může být i jeho soukromá e-mailová adresa. K doručování pracovněprávních písemností prostřednictvím služeb elektronických komunikací však může zaměstnavatel přistoupit pouze tehdy, vyslovil-li s tím zaměstnanec souhlas. Takto doručovaná písemnost musí být navíc podepsána ověřeným elektronickým podpisem a zaměstnanec musí její přijetí potvrdit zprávou podepsanou taktéž ověřeným elektronickým podpisem[152], ž čehož plyne, že využívání tohoto komunikačního kanálu jako oficiálního způsobu doručování písemností je v pracovněprávních vztazích zatím značně nepraktické.

– *údaje o vzdělání a předchozí praxi, popř. informace o zvláštních předpokladech či schopnostech*

Tyto údaje zaměstnavateli slouží k posouzení kvalit a vhodnosti uchazeče. Pro výkon některých povolání také právní předpisy stanoví minimální dosažené vzdělání.

– *osobní údaje rodičů*

Tyto údaje je zaměstnavatel oprávněn vyžadovat tehdy, hodlá-li zaměstnat nezletilého a rodiče jsou zákonnými zástupci tohoto zaměstnance.

V souvislosti s vyplňováním osobního dotazníku či jiným způsobením poskytování osobních údajů potenciálnímu zaměstnavateli se nabízí otázka možného postupu zaměstnavatele, pokud bude později zjištěno, že poskytnuté údaje jsou nesprávné. Zde bude rozhodující, zda byly ze strany uchazeče záměrně poskytnuty špatně ty údaje, které zaměstnavatel není oprávněn požadovat;

[151] Bartík, V., Janečková, E. *Ochrana osobních údajů v aplikační praxi.* 2. vyd. Praha: Linde, 2010, s. 159.

v takovém případě nesprávnost těchto údajů nemá žádný vliv na platnost následně uzavřené pracovní smlouvy, a to i kdyby tím uchazeč uvedl zaměstnavatele v omyl. Pokud by se však jednalo o informace, které je zaměstnavatel oprávněn před vznikem pracovního poměru vyžadovat, posuzovala by se taková situace dle ust. § 49a ObčZ. Pokud by tak zaměstnavatel uzavřel pracovní smlouvu v omylu, který by byl pro uzavření smlouvy rozhodný, a uchazeč tento omyl vyvolal nebo o něm alespoň musel vědět, byly by pracovní smlouva relativně neplatná[153].

6.2 Osobní spis zaměstnance

Mnoho osobních údajů svých zaměstnanců je zaměstnavatel nucen zpracovávat pro pozdější plnění zákonem stanovených povinností, a to zejména v oblasti sociálního zabezpečení a politiky zaměstnanosti. Zaměstnavatel má také povinnost vedení určité evidence o svých zaměstnancích (např. evidence pracovní doby a pracovní pohotovosti). Pro vybrané konkrétní obory nebo pracovní pozice jsou zaměstnavatelům uloženy povinnosti ve vztahu k evidenci zaměstnanců podrobněji; nalezneme je například v zákoně č. 258/2000 Sb., o ochraně veřejného zdraví, jenž v ustanovení § 40 stanoví povinnosti týkající se evidence rizikových prací.

Ustanovení § 312 ZP zaměstnavateli umožňuje (nikoli ukládá za povinnost) vést evidenci zpracovávaných osobních údajů ve formě osobního spisu zaměstnance[154], který tak bude představovat uceleným datovým souborem ve smyslu § 4 písm. m) Zákona[155]. Žádný předpis však již přesně nestanoví, které dokumenty mají být součástí takového spisu. Jeho obsah se odvíjí zásadně od potřeb a uvážení zaměstnavatele s přihlédnutím k jeho zákonným povinnostem. Určité dokumenty však obsahem spisu být nesmějí, a to buď z toho důvodu, že nejsou nezbytně nutné pro výkon práce a nijak s ním nesouvisejí (a zaměstnavatel

[152] § 335 ZP
[153] Dokument sub. pozn. č. 142, s. 136.
[154] Chládková, A. Osobní spis zaměstnance. *Personální a sociálně právní kartotéka.* 2008, č. 6, s. 4.

tedy takové údaje vyžadovat ani shromažďovat nesmí), nebo proto, že mají diskriminační povahu (a zaměstnavatel je nesmí v pracovněprávních vztazích zohledňovat, a není tedy ani důvod, aby je shromažďoval). Zaměstnavatel zároveň tyto informace nesmí získávat ani zprostředkovaně. Zaměstnavatelé by také neměli automaticky zakládat do spisu kopie všech listin, které jim zaměstnanec v souvislosti s pracovněprávním vztahem poskytne, neboť tyto dokumenty mohou obsahovat i další informace než pouze ty, které zaměstnavatel pro své účely potřebuje, resp. osobní údaje třetích osob. Součástí spisu by proto měly být jen ty dokumenty, které osvědčují informace uvedené v osobním dotazníku, a také ty, které přímo souvisí s pracovním poměrem[156].

Zákoník práce upravuje rovněž právo nahlížet do osobního spisu (§ 312 odst. 2 ZP). Je zejména dovoleno, aby do osobních spisů nahlíželi ti vedoucí zaměstnanci, kteří jsou konkrétním pracovníkům nadřízeni. Jak bude uvedeno dále, tito zaměstnanci jsou ohledně obsahu osobního spisu vázáni povinností mlčenlivosti; své nahlížecí právo navíc mohou využívat pouze v takové míře, která je nezbytná k plnění jejich povinností. Na základě novely zákoníku práce č. 365/2011 Sb. náleží právo nahlížet do osobního spisu výslovně také ÚOOÚ, přičemž za nahlížení se nepovažuje předložení jednotlivé písemnosti z tohoto spisu vnějšímu kontrolnímu orgánu, který si tuto písemnost vyžádá v souvislosti s předmětem kontroly prováděné u zaměstnavatele (zejména v souladu se zákonem č. 552/1991 Sb., o státní kontrole). Do spisu má přístup samozřejmě i dotčený zaměstnanec, jenž si z něho může pořizovat výpisky a kopie na náklady zaměstnavatele (§ 312 odst. 3 ZP), což souvisí i s právem subjektu na přístup ke zpracovávaným údajům ve smyslu § 12 Zákona.

Jak bylo uvedeno v předchozích odstavcích, osobní spis je v zásadě tvořen veškerou dokumentací, kterou zaměstnavatel z nějakého důvodu potřebuje pro výkon svých práv a povinností z pracovněprávního vztahu a která se vztahuje ke

[155] Janečková, E., Bartík, V. Vedení osobního spisu z pohledu ochrany osobních údajů. *Personální a sociálně právní kartotéka.* 2010, č. 7, s. 1.
[156] Tamtéž.

konkrétnímu zaměstnanci. Třídit tyto dokumenty je samozřejmě možné z více hledisek, přičemž nejobvyklejší bývá níže uvedené chronologické řazení[157]:

Dokumenty související s přijetím do pracovního poměru (včetně údajů zjištěných již před vznikem pracovněprávního vztahu)

- životopis zaměstnance
- osobní dotazník
- doklady o dosaženém vzdělání a dosavadní praxi
- potvrzení o zaměstnání (od bývalého zaměstnavatele) či podobné doklady od Správy sociálního zabezpečení (živil-li se zaměstnanec dříve jako osoba samostatně výdělečně činná) nebo úřadu práce (v případě přijetí nezaměstnaného)
- výpis z rejstříku trestů, je-li legitimně vyžadován (blíže viz subkapitola 6.3.2)
- doklad o vstupní lékařské prohlídce a doklad o příslušnosti ke zdravotní pojišťovně
- doklady o změněné pracovní způsobilosti
- doklady nezbytné pro výkon některých povolání (kopie řidičského průkazu, potravinářského průkazu atd.)
- pracovní smlouva, mzdový výměr, přehled pracovní náplně zaměstnance a další podobné dokumenty
- rozhodnutí orgánů státní správy (např. o přiznání důchodu, o invaliditě)

Dokumenty vzniklé v průběhu pracovního poměru

- dodatky k pracovní smlouvě a dalším dohodám
- doklady o prohlubování a zvyšování kvalifikace (např. kvalifikační dohoda dle § 234 an. ZP)
- dohody o neplaceném volnu a další písemné dohody mezi zaměstnancem a zaměstnavatelem

[157] Srov. dokument sub. pozn. č. 154, s. 5-6.

- evidence pracovní doby podle § 96 ZP
- vyúčtování cestovních náhrad, popř. doklady k jejich poskytnutí
- hodnocení (povinnost hodnotit práci podřízených je vedoucím zaměstnancům stanovena v ustanovení § 302 písm. a) ZP)
- písemné výtky
- doklady o převedení na jinou práci či přemístění do jiného místa výkonu práce
- souhlas zaměstnavatele s konkurenční činností dle § 304 ZP
- doklady o absolvování povinných školení, lékařských prohlídek atp.

Dokumenty související s ukončením pracovního poměru

- dokument, na jehož základ byl pracovní poměr ukončen (dohoda, výpověď, okamžité zrušení, zrušení ve zkušební době)
- kopie vydaného potvrzení o zaměstnání
- posudek o pracovní činnosti
- evidenční list důchodového pojištění

U větších zaměstnavatelů se značným počtem zaměstnanců některé dokumenty nemusejí být přímo součástí osobního spisu, ale mohou být vedeny dle předmětu souhrnně pro všechny zaměstnance (např. dokumentace v oblasti BOZP či předávací protokoly ke služebním vozidlům).

Jak zde již bylo několikrát zmíněno, řadu osobních údajů je zaměstnavatel povinen zpracovávat v souvislosti se sociálním zabezpečením zaměstnanců. Tak například zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení ukládá v ustanovení § 37 zaměstnavateli povinnost týkající se evidence pro účely důchodového pojištění. Tato zaměstnavatelem vedená evidence musí obsahovat příjmení (včetně všech dřívějších příjmení), jméno, datum a místo narození, místo trvalého pobytu, státní občanství, rodné číslo, informaci o tom, zda je zaměstnanec poživatelem starobního či invalidního důchodu a další údaje o konkrétním pracovněprávním vztahu.

Kromě údajů, které zaměstnavatel získal již před vznikem pracovněprávního vztahu, je tak zaměstnavatel navíc oprávněn zpracovávat i bez souhlasu zaměstnanců[158] následující údaje (přestože v době před vznikem pracovního poměru nebyl zaměstnavatel dle § 30 odst. 2 ZP oprávněn tyto údaje od zaměstnance požadovat, nyní je pro něj jejich znalost nezbytná pro plnění zákonem stanovených povinností):

– *rodné číslo, místo narození*

Používání rodného čísla je upraveno v zákoně č. 133/2000 Sb., o evidenci obyvatel. Ten ve svém ustanovení § 13c odst. 1 písm. c) stanoví, že rodné číslo je možné používat výhradně se souhlasem jeho nositele, resp. že nakládat s rodným číslem je oprávněna pouze fyzická osoba, jíž bylo rodné číslo přiděleno, popř. její zákonný zástupce. V pracovněprávních vztazích tedy platí, že pokud zaměstnanec své rodné číslo zaměstnavateli pro jeho potřeby poskytne, je jeho uvádění v pracovněprávních dokumentech přípustné. Jelikož však rodné číslo není uvedeno v § 4 písm. b) Zákona, nejedná se o citlivý údaj[159] a není tak pro jeho zpracování nezbytný výslovný souhlas subjektu[160]. Nesmíme však opomenout ani ustanovení § 13c odst. 1 písm. b) výše zmíněného zákona, podle něhož lze rodné číslo využívat také tehdy, stanoví-li tak zvláštní zákon, což v pracovněprávních vztazích v souvislosti s oblastí sociálního zabezpečení není neobvyklé[161]. Místo narození musí zaměstnavatel uvádět na evidenčních listech zasílaných na správu sociálního zabezpečení[162].

– *bydliště (trvalé i přechodné)*

[158] Na základě zákonné výjimky dle ustanovení § 5 odst. 2 písm. a) ZOOÚ.
[159] Kučerová, A. Nonnemann, F. *Ochrana osobních údajů v otázkách a odpovědích.* 1. vyd. Praha: BOVA POLYGON, 2010, s. 13.
[160] Opačný názor lze však nalézt např. v publikaci H. D´Ambrosové *Ochrana osobních údajů v personalistice od roku 2005*, 1. vyd., s. 28.
[161] Je však nesporné, že potřeba zaměstnavatele zpracovávat rodné číslo vzniká až při vzniku pracovního poměru, tzn. zaměstnavatel by zásadně neměl zpracovávat rodná čísla uchazečů o zaměstnání. Srov. též Stanovisko WP 48 o zpracování osobních údajů v souvislosti se zaměstnáváním, s. 18.
[162] Srov. například § 22 písm. a) nebo § 37 zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení.

Znalost bydliště je pro zaměstnavatele nutná kupříkladu ve vztahu k doručování pracovněprávních písemností, nepodaří-li se je zaměstnanci doručit na pracovišti (§ 334 odst. 1 ZP). Od místa bydliště se také odvíjí některé nároky zaměstnanců (zejména cestovní náhrady) či možnost vysílání zaměstnanců na pracovní cesty (§ 240 odst. 1 ZP).

– *státní příslušnost*

Znalost této informace je pro zaměstnavatele důležitá zejména tehdy, je-li zaměstnancem cizinec či osoba bez státní příslušnost, neboť v takovém případě existuje i další způsob skončení pracovního poměru zaměstnancem, a to dle ustanovení § 48 odst. 3 zákoníku práce (tj. zejména uplynutím doby povolení k pobytu či zaměstnání). Zaměstnavatel má rovněž povinnost vést evidenci cizinců, kteří jsou u něj zaměstnáni, a rovněž také informační povinnost vůči úřadu práce[163].

– *informace o zdravotní pojišťovně*

Tuto informaci je zaměstnanec povinen sdělit svému zaměstnavateli nejpozději v den nástupu do zaměstnání. Zaměstnavatel má dokonce právo požadovat na zaměstnanci úhradu penále, které zaplatí v souvislosti s neoznámením, resp. opožděným oznámením změny zdravotní pojišťovny[164]. Zdravotní pojišťovně zaměstnance musí zaměstnavatele oznamovat nástup zaměstnance do zaměstnání a ukončení tohoto zaměstnání, jakož i případnou změnu zdravotní pojišťovny či nástup na mateřskou nebo rodičovskou dovolenou a její ukončení, a to do osmi dnů ode dne předmětné události.

– *údaj o tom, zda je zaměstnanec poživatelem některého typu důchodu*

[163] § 102 odst. 2 a § 87 an. ZZ
[164] Srov. § 12 písm. b) zákona č. 48/1997 Sb., o veřejném zdravotním pojištění.

Tento údaj je pro zaměstnavatele významný v souvislosti se správným výpočtem měsíčních záloh na daň z příjmů, kterou je povinen ze mzdy zaměstnance odvádět[165].

– *posudek o zdravotním stavu, informace o zdravotním postižení*

Pro zabezpečení bezpečnosti a ochrany zdraví při práci je nutné, aby měl zaměstnavatel informaci o tom, zda je zaměstnanec práce schopen či ne, případně zda u něj existují nějaká omezení a zda je potřeba mu přizpůsobit pracovní podmínky[166]. Pozbude-li zaměstnanec během trvání pracovního poměru vzhledem ke svému zdravotnímu stavu způsobilost konat dále dosavadní práci, má zaměstnavatel možnost (v některých případech dokonce povinnost) jej převést na jinou práci. Zaměstnavatelé s více než 25 zaměstnanci v pracovním poměru navíc potřebují tuto informaci znát ve vztahu k plnění povinného podílu zaměstnávání osob se zdravotním postižením[167].

– *údaje o vzdělání a předchozí praxi*

Tyto údaje často slouží ke správnému výpočtu odměny (především platu) a pro zaměstnavatele jsou rovněž významné v souvislosti s povinností zaměstnavatele poskytovat všem zaměstnancům za stejnou práci nebo práci stejné hodnoty stejnou mzdu nebo plat, přičemž stejnou prací se rozumí práce srovnatelné složitosti, namáhavosti a odpovědnosti, což se posuzuje dle dosaženého vzdělání a dalších znalostí či dovedností[168].

– *zjištění další činnosti zaměstnance shodné s předmětem činnosti zaměstnavatele podle § 304 ZP*[169]

– *údaj o členství ve výboru odborové organizace*

[165] Srov. též Výroční zpráva ÚOOÚ za rok 2007, s. 20.
[166] § 103 ZP
[167] Tento podíl činí k dnešnímu dni 4% - srov. § 81, resp. § 83 ZZ.
[168] § 110 ZP. Srov. též Výroční zpráva ÚOOÚ za rok 2007, s. 20.
[169] Dokument sub. pozn. č. 150, s. 32.

Zaměstnavatel nesmí zjišťovat, kdo je a kdo není členem odborové organizace (tato informace je citlivým údajem dle § 4 písm. b) Zákona). Protože však členům *výboru* odborové organizace poskytuje zákoník práce zvýšenou ochranu před výpovědí, má právo zaměstnavatel vědět, kdo ze zaměstnanců je odborovým funkcionářem[170].

Aby si zaměstnavatel mohl být jist, že zpracovává skutečně aktuální údaje svých zaměstnanců, může jim například každoročně poskytovat přehled údajů, které zpracovává, aby tak sami mohli zkontrolovat jejich přesnost a pravdivost[171]. Všechny výše uvedené údaje je přitom zaměstnavatel oprávněn zpracovávat bez souhlasu zaměstnanců a jeho požadování od zaměstnanců je tak nadbytečná procedura. Je zapotřebí, aby si zaměstnavatelé uvědomili, že zpracování takových údajů, které od zaměstnanců požadovat nesmí, nezlegitimní souhlasem zaměstnance s jejich zpracováním[172]. V mnoha případech zaměstnanci souhlas udělí ve strachu před ztrátou zaměstnání či „znelíbení“ se zaměstnavateli. Posouzení dobrovolnosti poskytnutí souhlasu proto bude v pracovněprávních vztazích vždy problematické.

6.2.1 Údaje o rodinných příslušnících

V souvislosti s některými povinnostmi stanovenými zákonem je zaměstnavatel oprávněn zpracovávat následující údaje o rodinných příslušnících, a to aniž by bylo nutné žádat zaměstnance o souhlas s jejich zpracováním:

– *údaje o dětech zaměstnance*

Zaměstnavatel je oprávněn požadovat informace (jméno, příjmení a rodné číslo) o dětech zaměstnance, a to nejen těch, kteří se zaměstnancem žijí ve společné domácnosti (pro účely stanovení starobního důchodu je rozhodující počet všech *vychovaných* dětí). S údaji o dětech souvisí také řada povinností zaměstnavatele, a to zejména v souvislosti s ochranou těhotných zaměstnankyň a rodičů malých dětí

[170] Tamtéž.
[171] Stanovisko WP 48 o zpracování osobních údajů v souvislosti se zaměstnáváním, s. 22.

(mateřská a rodičovská dovolená, vysílání na pracovní cestu, zákaz výpovědi dané zaměstnavatelem a další). V případě, kdy zaměstnavatel hodlá zpracovávat osobní údaje dětí zaměstnanců v rozsahu větším, než mu ukládají právní předpisy, nabízí se otázka, kdo by měl udělit souhlas k jejich zpracování. Podle § 9 občanského zákoníku mají nezletilí (tj. mladší osmnácti let) způsobilost jen k takovým úkonům, které jsou svou povahou přiměřené rozumové a volní vyspělosti odpovídající jejich věku. V případě souhlasu se zpracováním vlastních osobních údajů se dá předpokládat, že k jeho udělení by měl jedinec být v zásadě způsobilý od 15ti let věku. U mladších osob by potom bylo vhodné, aby souhlas udělil druhý ze zákonných zástupců, neboť v případě zaměstnance potenciálně hrozí střet zájmů mezi zájmem vlastním a zájmem dítěte[173].

– *rodinný stav a údaje o manželovi (partnerovi)*

Znalost tohoto údaje (jméno a příjmení, název a adresu zaměstnavatele druhého z manželů) potřebuje zaměstnavatel tehdy, zpracovává-li pro zaměstnance prohlášení poplatníka daně z příjmu fyzických osob (v souladu se zákonem č. 586/1992 Sb., o daních z příjmů), pro určení výše cestovních náhrady v souvislosti s návštěvou rodiny a také pro případné nároky v souvislosti s úmrtím zaměstnance[174].

6.2.2 Archivace osobního spisu

Se zpracováním osobních údajů také samozřejmě souvisí archivace osobního spisu po ukončení pracovněprávního vztahu a následná likvidace údajů. Ani v tomto případě není předepsaná jednotná lhůta, po jakou dobu po skončení pracovního či obdobného poměru je zaměstnavatel povinen obsah osobního spisu archivovat. Různé právní předpisy stanoví odlišně dlouhé lhůty a u každého

[172] Tamtéž.
[173] Viz také rozhodnutí ÚOOÚ čj. 7/05/SŘ-OSČ.
[174] § 375 an. ZP

dokumentu je tak nutné zvažovat, do které skupiny patří a jak dlouho je třeba jej uchovávat. Právní úprava je přitom v této oblasti velmi roztříštěná[175]:

Například dle zákona č. 563/1991 Sb. o účetnictví, a to konkrétně ustanovení § 31 odst. 2, je nutné účetní záznamy, mezi něž patří i evidence přesčasů či daňové doklady, uchovávat po dobu alespoň pěti let počínaje koncem účetního období, kterého se týkají. Je-li vedeno jakékoliv správní či soudní řízení, pro které mohou mít dané doklady význam, je nezbytné tyto dokumenty archivovat až do skončeného daného řízení, a to i po uplynutí výše uvedené lhůty.

V souladu se zákonem č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení (konkrétně ustanovení § 35a odst. 4) jsou zaměstnavatelé povinni uschovávat evidenční listy důchodového pojištění po dobu tří let po roce, kterého se týkají, a mzdové listy a účetní záznamy o údajích potřebných pro účely důchodového zabezpečení po dobu třiceti let následujících po roce, kterého se týkají (u poživatelů starobního důchodu po dobu deseti let). Podle ustanovení § 96 zákona č. 187/2006 Sb., o nemocenském pojištění musí zaměstnavatel dále uschovávat záznamy pro účely nemocenského pojištění (jako jsou např. doklady o vzniku a skončení pracovněprávního vztahu či evidence docházky) po dobu deseti let.

6.3 Možnost zpracování citlivých údajů zaměstnanců

Pro shromažďování a zpracovávání tzv. citlivých údajů stanoví Zákon přísnější režim. O případech, kdy a za jakých podmínek je správce na základě ustanovení § 9 Zákona oprávněn citlivé údaje zpracovávat, již bylo pojednáno výše v subkapitole 2.3, proto se na tomto místě zaměřím na specifické problémy při zpracovávání citlivých údajů v pracovněprávních vztazích. Z citlivých údajů zaměstnavatelé přitom nejčastěji zpracovávají zejména údaje o zdravotním stavu zaměstnance, údaje o případné trestné činnosti a fotografii zaměstnance, která může, avšak nemusí být nosičem citlivého údaje.

[175] Dokument sub. pozn. č. 154, s. 7.

6.3.1 Informace o zdravotním stavu

Jelikož zaměstnavatel nesmí na základě ustanovení § 103 odst. 1 písm. a) ZP připustit, aby zaměstnanec vykonával práce, jejichž náročnost by neodpovídala jeho schopnostem a zdravotní způsobilosti, je evidentní, že je oprávněn od svých zaměstnanců vyžadovat lékařský posudek potvrzující, že mohou vykonávat práci sjednanou v pracovní smlouvě či dohodě o práci konané mimo pracovní poměr. Zaměstnanec je navíc povinen podrobit se preventivním prohlídkám a dalším lékařským vyšetřením[176]. Pokud však lékařský posudek neobsahuje žádné konkrétní údaje o zdravotním stavu zaměstnance, nýbrž se omezuje na pouhé konstatování, že zaměstnanec je způsobilý vykonávat sjednaný druh práce, nebude se jednat o citlivý údaj zaměstnance[177].

Citlivé údaje o zdravotním stavu zaměstnanců je v zásadě oprávněn zpracovávat např. smluvní závodní lékař, nikoliv ovšem zaměstnavatel[178], neboť se jedná o předmět lékařského tajemství. S citlivým údajem o zdravotním stavu zaměstnance se tak zaměstnavatel může setkat jedině v případě, že mu jej zaměstnanec sám bez vyzvání poskytne, a to kupříkladu pokud bude vyžadovat převedení na jinou práci dle ustanovení § 41 ZP odst. 1 ZP (například pokud se u zahradníka rozvine pylová alergie, přičemž doloží lékařským posudkem nezpůsobilost nadále vykonávat původní druh práce, a bude požadovat převedení na kancelářskou práci). Stejně tak bude zaměstnavatel seznámen s informacemi o zdravotním stavu zaměstnance v případě pracovního úrazu či nemoci z povolání a také tehdy, dozví-li se o těhotenství zaměstnankyně. Přesto i v případě, kdy zaměstnanec údaje o svém zdravotním stavu zaměstnavateli poskytne sám od sebe, nesmí je zaměstnavatel zpracovávat bez dalšího (např. založit do osobního spisu zaměstnance), aniž by si k tomu vyžádal informovaný a výslovný souhlas zaměstnance podle ustanovení § 9 Zákona. Tento souhlas by měl poté uchovávat

[176] § 106 odst. 4 písm. b) ZP
[177] Dokument sub. pozn. č. 151, s. 165.
[178] ÚOOÚ k problémům z praxe č. 2/2005 – Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů.

spolu s dokladem obsahujícím tento citlivý údaj tak, aby jeho udělení mohl případně prokázat[179].

6.3.2 Údaje o případné trestné činnosti

I v tomto případě je nutné vyjít z ustanovení § 316 odst. 4 ZP, podle něhož zaměstnavatel nesmí vyžadovat od zaměstnance informace, které bezprostředně nesouvisejí s výkonem práce a s pracovněprávním vztahem. Proto také nesmí od zaměstnance vyžadovat informaci o trestněprávní bezúhonnosti, ledaže by pro to byl dán věcný důvod spočívající v povaze práce, která má být vykonávána, a je-li tento požadavek přiměřený. Skutečnost, zda zaměstnanec či uchazeč o zaměstnání byl v minulosti trestán, se bude zpravidla prokazovat výpisem z rejstříku trestů (TR). V praxi se přitom považuje za odůvodněné, je-li výpis z TR vyžadován kupříkladu od zaměstnanců majících přístup k větším finančním obnosům či nebezpečným látkám nebo od profesionálních řidičů či strážných objektů. Zákon může také stanovit případy, kdy je vyžádání si výpisu z trestního rejstříku přímo povinností zaměstnavatele[180].

Výpis z trestního rejstříku může za výše uvedených podmínek zaměstnavatel vyžadovat jak před uzavřením pracovněprávního poměru, tak během jeho trvání. Pro tyto případy by však bylo vhodné, aby zaměstnavatel upravil vnitřním předpisem, pro které pozice a za jakých podmínek je od zaměstnanců výpis z TR vyžadován (např. jak často; dle mého názoru lze jako přijatelnou akceptovat minimální lhůtu pro opakovaný výpis jeden rok). Stejně tak je možné vnitřním předpisem zakotvit požadavek bezúhonnosti jako podmínku zastávání konkrétní pozice. Ve všech případech by však měl zaměstnavatel své požadavky přiměřeně odůvodnit. Nově přijatý vnitřní předpis stanovící podmínku bezúhonnosti by se však vždy měl vztahovat pouze k zaměstnancům přijatým na danou pozici až během účinnosti tohoto předpisu. V opačném případě by totiž tohoto mohlo být

[179] Srov. dokument sub. pozn. č. 150, s. 25.
[180] § 6 odst. 4 písm. b) zákona č. 312/2002 Sb., o úřednících územně samosprávných celků, ve znění pozdějších předpisů

využíváno za účelem zbavení se nežádoucích zaměstnanců při neexistenci zákonného výpovědního důvodu dle zákoníku práce, a tedy obcházení zákona.

V současnosti mezi odbornou veřejností převládá názor, že pouhý výpis z rejstříku trestů obsahující informaci, že v něm daná osoba nemá záznam, není citlivým údajem ve smyslu ustanovení § 4 písm. b) Zákona, neboť takový výpis neobsahuje žádnou informaci o konkrétním odsouzení za trestný čin a je pouze dokladem trestní bezúhonnosti[181]. Citlivým údajem je tedy jen údaj vypovídající o odsouzení konkrétní osoby za spáchaný trestný čin, ať už konkrétními údaji o odsouzení či pouhou informací, že daná osoba odsouzena byla (např. informace „Má záznam v rejstříku trestů."). Výpis či opis z TR obsahující takovou informaci je potom samozřejmě nutné pokládat za citlivý údaj a jako s takovým s ním nakládat[182]. Nabízí se však otázka, zda citlivým údajem (a nikoliv „pouze" osobním údajem) bude informace o trestním stíhání dotyčné osoby, neboť Zákon hovoří pouze o *odsouzení* za trestný čin, nikoliv trestním stíhání za něj. Vzhledem k principu presumpce neviny se kloním k názoru, že spíše nikoliv. Na druhou stranu je však třeba v souladu s nálezem Ústavního soudu sp.zn. II. ÚS 82/07, jenž odkazuje mimo jiné na judikaturu Evropského soudu pro lidská práva[183] vycházející z materiálního chápání pojmu trestní obvinění a podřazující tak pod pojem *trestní* obvinění a odsouzení také obvinění a potrestání za přestupek či další správní delikt, chápat pod pojmem *odsouzení za trestný čin* rovněž jako údaj o odsouzení za správní delikt[184]. Znovu nám však zde vyvstává další otázka – zahrnuje pojem *odsouzení* i udělení sankce ve správním řízení? Je tak citlivým údajem kupříkladu Výpis z registru řidičů o záznamech bodového hodnocení řidiče?

Na základě informace získané z výpisu z TR se může zaměstnavatel rozhodnout, uzavře-li s uchazečem pracovní poměr. Důsledky však lze vyvodit i

[181] Srov. např. dokument sub. pozn. č. 159, s. 20.
[182] Srov. dokument sub. pozn. č. 150, s. 39.
[183] Rozsudek Evropského soudu pro lidská práva ve věci Özturk proti Německu ze dne 21.2.1984 či rozsudek téhož soudu ve věci Lauko proti Slovensku ze dne 2.9.1998.

pro stávající zaměstnance, a to jednak na základě vnitřního předpisu (jak uvedeno výše), kdy zaměstnanec ztrátou své bezúhonnosti přestane splňovat požadavky pro řádný výkon své práce a je tedy dán výpovědní důvod dle § 52 písm. f) ZP, a jednak na základě zákoníku práce. Byl-li totiž zaměstnanec pravomocně odsouzen pro úmyslný trestný čin k nepodmíněnému trestu odnětí svobody na dobu delší než 1 rok, nebo byl-li pravomocně odsouzen pro úmyslný trestný čin spáchaný při plnění pracovních úkolů nebo v přímé souvislosti s nimi k nepodmíněnému trestu odnětí svobody na dobu nejméně 6 měsíců, může zaměstnavatel využít možnosti, kterou mu poskytuje ustanovení § 55 odst. 1 písm. a) ZP, a okamžitě pracovní poměr zrušit. V tomto případě však zaměstnavatel musí zrušit pracovní poměr nejpozději do 2 měsíců ode dne, kdy mu byl výpis z TR předložen a zároveň tomu tak nesmí být později než 1 rok ode dne vydání pravomocného odsuzujícího rozsudku (§ 58 ZP).

6.3.3 Fotografie

Posledním častým „údajem“, který od zaměstnanců či uchazečů zaměstnanci vyžadují, je předložení průkazové fotografie. To, zda lze fotografii zaměstnance považovat za dokument obsahující citlivý údaj, bude záležet především na tom, jaké informace z ní lze vyčíst a zejména za účelem zjištění jakých informací je fotografie pořizována. Fotografie může vypovídat o rasovém nebo etnickém původu vyobrazené osoby či dokonce o jejím postižení, a tedy o zdravotním stavu. V závislosti na úrovni použitých technologií je dokonce možné z některých fotografií získat biometrické údaje dotyčné osoby[185]. Jestliže však bude fotografie pořízena a uchovávána pouze za účelem rozlišení jedné osoby od druhé, bude nakládání s ní podřízeno režimu „obvyklých“ osobních údajů, nikoli údajů citlivých[186]. Aby takové zpracování údajů navíc podléhalo i režimu Zákona, musí se jednat o zpracování nikoliv nahodilé; v opačném případě se nakládání s fotografiemi bude řídit zejména ustanoveními občanského zákoníku.

---

[184] Srov. též Bartík, V., Janečková, E. *Zákon o ochraně osobních údajů s komentářem.* 1. vyd. Olomouc: ANAG, 2010, s. 39.
[185] Viz dokument sub. pozn. č. 159, s. 12.
[186] ÚOOÚ k problémům z praxe č. 3/2010 – K použití fotografie, obrazového a zvukového záznamu fyzické osoby.

Obecně lze při pořizování fotografií či podobného obrazového záznamu rozlišovat trojí režim:

a) pořízení jednotlivých fotografií v běžném životě (např. na firemním večírku). V tomto případě je k pořízení a použití fotografie nutné svolení snímané osoby v souladu s ustanovením § 12 odst. 1 ObčZ (za svolení je přitom možné považovat i skutečnost, že dotyčná osoba fotografovi pózuje), jinak pouze na základě tzv. zákonné licence (úřední účely, vědecké a umělecké účely, zpravodajství). Pokud jsou tyto fotografie označeny názvem akce a nikoli údaje, na základě nichž by bylo možné identifikovat jednotlivé subjekty údajů, nepodléhá jejich pořizování Zákonu[187], a tedy ani oznamovací povinnosti podle § 16 Zákona.

b) bude-li však docházet k systematickému pořizování obrazových záznamů konkrétní fyzické osoby, musí takovéto pořizování snímků probíhat v souladu se Zákonem (a podpůrně samozřejmě také občanským zákoníkem).

c) jestliže navíc budou snímky pořizovány za účelem dalšího zpracování citlivých údajů v nich obsažených (např. rasový či etnický původ), bude k jejich pořizování a dalšímu zpracování zapotřebí výslovného souhlasu subjektu (respektive jedné ze Zákonných výjimek) [188].

V případech, kdy zaměstnavatel fotografii zaměstnance požaduje za účelem vydání služebního průkazu, jehož vydání mu ukládá zákon, bude se jednat o zpracování ve smyslu ustanovení § 5 odst. 2 písm. a) Zákona, neboť vydání tohoto průkazu obsahujícího fotografii zaměstnance je nezbytné k dodržení právní povinnosti zaměstnavatele. V těchto případech proto ke zpracování fotografie není zapotřebí souhlasu zaměstnance. Jakékoliv další využití fotografie (např. umístění na webových stránkách zaměstnavatele) je však již podmíněno poskytnutím souhlasu ze strany zaměstnance a také splněním oznamovací povinnosti vůči Úřadu[189].

[187] Dokument sub. pozn. č. 151, s. 203.
[188] ÚOOÚ k problémům z praxe č. 3/2010 – K použití fotografie, obrazového a zvukového záznamu fyzické osoby.
[189] Dokument sub. pozn. č. 151, s. 167.

6.4 Poskytování informací o zaměstnancích, jejich zveřejňování na internetu a povinnost mlčenlivosti

V souvislosti s poskytováním informací o zaměstnancích bývá v praxi problém s uváděním kontaktních údajů na jednotlivé zaměstnance na internetových stránkách zaměstnavatele. Takové zveřejňování[190] je totiž zpracování osobních údajů ve smyslu ustanovení § 4 písm. e) Zákona a nabízí se tedy otázka, zda je k němu zapotřebí souhlasu zaměstnance. Dle názoru Úřadu zveřejněného ve Věstníku č. 18/2002 se na takové uveřejňování údajů o zaměstnancích bude vztahovat zákonná výjimka (podle § 5 odst. 2 písm. e) Zákona, na jejímž základě je možné zpracovávat údaje i bez souhlasu subjektu, je-li to nezbytné pro ochranu práv a právem chráněných zájmů správce. Oprávněný zájem správce v tomto případě představuje zájem a potřeba zaměstnavatele informovat stávající i potenciální klienty a obchodní partnery o kontaktních osobách a jejich postavení u zaměstnavatele, na něž se mohou v případě zájmu obrátit. Uveřejnění těchto kontaktních údajů je tak nezbytné pro zajištění ekonomických zájmů zaměstnavatele, neboť bez jejich uspokojování by svou činnost nemohl efektivně vyvíjet. Pokud bychom tuto situaci dovedli ad absurdum, bez uveřejňování některých údajů o zaměstnancích by se tito zaměstnanci stali nadbytečnými, neboť by zaměstnavatelovy hospodářské výsledky byly v důsledku nemožnosti efektivního řízení tak nízké, že by se mu jeho podnikatelská činnost nevyplatila. Na druhou stranu však samozřejmě i zde platí, že takové uveřejňování údajů nesmí být v rozporu s ochranou soukromého a osobního života zaměstnance. Zaměstnavatel tedy nemá právo uvádět na internetu (respektive jakkoliv jinak zveřejňovat, například prostřednictvím podnikového časopisu) soukromé telefonní číslo zaměstnance, jeho rodinný stav, počet dětí a další (pro klienty či

[190] V tomto případě se samozřejmě nejedná o zveřejňování ve smyslu § 769 zákona č. 513/1991 Sb., Obchodní zákoník, ve znění pozdějších předpisů, kde „zveřejněním" je rozuměno zveřejnění v Obchodním věstníku, neboť na rozdíl od obchodního zákoníku ZOOÚ nerozlišuje mezi zveřejněním a uveřejněním.

spolupracovníky nadbytečné) osobní údaje[191]. Výjimku představuje situace, kdy k takovému uveřejnění dá zaměstnanec zaměstnavateli souhlas, jelikož má na zveřejnění těchto údajů svůj vlastní zájem.

Za podobný případ, kdy je zaměstnavatel oprávněn poskytnout osobní údaje svých zaměstnanců třetím osobám, aniž by k tomu měl jejich souhlas, je dle mého názoru možné považovat i situaci, kdy zaměstnavatel pověří kontrolou dodržování režimu práce neschopného ze strany zaměstnance externí subjekt (např. detektivní kancelář), přičemž mu za tímto účelem předá i osobní údaje o zdravotním stavu dotyčného zaměstnance (logicky nejméně informaci o skutečnosti, že je zaměstnanec krátkodobě práce neschopným). I v tomto případě se na takový postup aplikuje zákonná výjimka, neboť takové zpracování je nezbytné k ochraně oprávněných zájmů zaměstnavatele. Nelze totiž po zaměstnavateli spravedlivě žádat, aby tyto kontroly během prvních 21 kalendářních dnů trvání pracovní neschopnosti, kdy je povinen od 4. dne pracovní neschopnosti zaměstnanci poskytovat náhradu mzdy[192], prováděl výhradně sám, popřípadě prostřednictvím svých zaměstnanců. Od 1.1.2012 k tomuto navíc nově přistoupilo právo zaměstnavatele, upravené v ust. § 52 písm. h) zákoníku práce[193], umožňující zaměstnavateli ukončit pracovní poměr zaměstnance výpovědí při porušení režimu dočasné pracovní neschopnosti zvlášť hrubým způsobem.

V praxi vznikají také problematické situace ve vztahu k poskytování informace o výši mzdy zaměstnance, a to nejčastěji v souvislosti s poskytováním úvěrů. Zaměstnanec v pozici žadatele o úvěr obvykle sám po zaměstnavateli požaduje potvrzení výše svých příjmů na formuláři vydaném úvěrovou institucí. Jestliže však pracovníci této instituce zaměstnavatele poté kontaktují a znovu žádají o ověření údaje, dostává se zaměstnavatel do prekérní situace, neboť není oprávněn tento osobní údaj nikomu sdělit. Předložení formuláře se samozřejmě dá

[191] Srov. též Mokrý, L. Uvedení jmen zaměstnanců na firemních stránkách vs. ochrana osobních údajů, dostupný z www.pravoit.cz/article/uvedeni-jmen-zamestnancu-na-firemnich-strankach-vs-ochrana-osobnich-udaju.
[192] § 192 ZP
[193] Zavedené novelou zákoníku práce č. 365/2011 Sb.

považovat za konkludentní souhlas zaměstnance s poskytnutím tohoto údaje dané instituci, ovšem v případě telefonického či koneckonců i e-mailového dotazu ze strany finanční společnosti nemá zaměstnavatel možnost identitu tazatele ověřit[194]. V těchto situacích zaměstnavatelé obvykle postupují tak, že výši příjmu zaměstnance tázající osobě potvrdí (tzn., potvrdí konkrétní částku), přesnou výši však nesdělí. Jak zaměstnanci, tak tázající se instituce by si však měli uvědomit, že i tímto postupem zaměstnavatel striktně vzato porušuje své povinnost správce stanovené Zákonem[195].

S poskytováním a zpřístupňování údajů zaměstnance také úzce souvisí povinnost mlčenlivosti všech ostatních zaměstnanců a jiných fyzických osob, které přijdou s těmito údaji do styku, jež trvá i po zániku pracovního či jiného smluvního vztahu k zaměstnavateli. Povinnost mlčenlivosti ve vztahu k osobním údajům zaměstnanců není v zákoníku práce výslovně stanovena[196]. Její absence je překlenuta stanovením výčtu osob oprávněných nahlížet do osobního spisu zaměstnance a také ustanovením § 314 odst. 2 zákoníku práce, které stanoví, že zaměstnavatel nesmí poskytovat o zaměstnanci jiné informace, než které mohou být obsahem pracovního posudku, bez jeho svolení. Zákoník práce také vyjmenovává konkrétní případy zachovávání mlčenlivosti o důvěrných informacích, a to pro členy odborové organizace, rady zaměstnanců a zástupce pro oblast bezpečnosti a ochrany zdraví při práci a odborníkům, které si přizvou[197], a také zaměstnanců veřejné správy[198]. Na zpracování osobních údajů zaměstnanců se však samozřejmě vztahuje i ustanovení § 15 Zákona obsahující povinnost zachovávání mlčenlivosti také všem zaměstnancům správce nebo zpracovatele, a to nejen ve vztahu k obsahu těchto údajů, ale rovněž ve vztahu k bezpečnostním opatřením, která se jich týkají. Za porušení mlčenlivosti však může zaměstnavatel zaměstnance postihnout pouze prostředky, které mu poskytuje zákoník práce.

[194] Srov. dokument sub. pozn. č. 151, s. 183.
[195] Srov. dokument sub. pozn. č. 159, s. 58.
[196] Bartík, V., Janečková, E. Poskytování osobních údajů o zaměstnancích. *Práce a mzda.* 2010, č. 10, s. 22.
[197] § 276 odst. 3 a 4 ZP
[198] § 303 odst. 1 a 2 ZP

Porušení povinnosti mlčenlivosti se bude posuzovat jako porušení povinností vyplývajících z právních předpisů vztahujících se k zaměstnancem vykonávané práci a jako takové může v závislosti na okolnostech představovat výpovědní důvod v souladu s ustanoveními § 52 písm. f) nebo g) či § 55 odst. 1 písm. b) ZP[199]. Porušením povinnosti mlčenlivosti se však zaměstnanec zároveň dopustí přestupku dle § 44 odst. 1 Zákona; pracovní poměr ke správci nebo zpracovateli ale není podmínkou pro odpovědnost za tento přestupek[200].

Právě okamžitým zrušením pracovního poměru pro porušení povinnosti mlčenlivosti ze strany zaměstnance se zabýval Nejvyšší soud ve svém rozsudku sp.zn. 21 Cdo 2633/2008 ze dne 2.7.2009. V posuzovaném případě zaměstnankyně vykonávala pro zaměstnavatele působícího v oblasti veřejné správy práci mzdové účetní a přicházela tak do styku s osobními spisy zaměstnanců a dalších osob. Tato zaměstnankyně se obrátila na příslušný úřad práce se stížností na nesprávné zařazení své osoby a potažmo i dalších osob do platových tříd a jako důkaz ke svému podání připojila kopie pracovních náplní uvedených osob obsahující rovněž údaje o výši jejich platu. Po zjištění této skutečnosti s ní zaměstnavatel okamžitě rozvázal pracovní poměr ve smyslu § 53 odst. 1 písm. b) tehdy platného zákoníku práce (zákon č. 65/1965 Sb.), a to pro porušení pracovní kázně zvlášť hrubým způsobem, jež spatřoval v porušení povinnosti mlčenlivosti stanovené jak zákoníkem práce, tak vnitřními předpisy zaměstnavatele. Prvoinstanční soud žalobu na neplatnost okamžitého zrušení zamítl, odvolací soud však žalobě vyhověl. Nejvyšší soud se ve svém rozsudku ztotožnil s argumentací odvolacího soudu a shodně uvedl, že pro posouzení míry porušení pracovní kázně ve vztahu k povinnosti mlčenlivosti je nezbytné přihlédnout k tomu, komu byly údaje poskytnuty (zde kontrolnímu orgánu, který je rovněž povinen zachovávat mlčenlivost), za jakým účelem (propuštěna zaměstnankyně se domáhala ochrany svých práv) a jaká újma tímto porušením vznikla, a okamžité rozvázání pracovního

[199] Srov. též Randlová, N. Váňová, L. Povinnost zachovávat mlčenlivost v pracovněprávním vztahu a ochrana osobních údajů ostatních zaměstnanců. *Personální a sociálně právní kartotéka.* 2009, č. 10, s. 23.
[200] Srov. dokument sub. pozn. č. 196, s. 23.

poměru v tomto případě označil za neplatné, neboť porušení mlčenlivosti stanovené v § 15 odst. 1 Zákona a tedy porušení pracovní kázně nedosahovalo zákoníkem práce požadované míry závažnosti[201].

6.5 Likvidace osobních údajů zaměstnanců

Likvidací osobních údajů rozumíme poslední etapu jejich zpracování, což lze odvodit ze znění ustanovení § 4 písm. e) Zákona, které mezi příkladmým výčtem druhů zpracovávání osobních údajů zahrnuje rovněž jejich likvidaci. Písmeno i) téhož paragrafu poté uvádí, že likvidací údajů se rozumí fyzické zničení jejich nosiče (např. skartace spisů), jejich fyzické vymazání (např. začernění) nebo jiné trvalé vyloučení z dalšího zpracování, přičemž jejím cílem je znemožnění jakéhokoliv dalšího zpracovávání těchto osobních údajů, tj. včetně „pouhého" uchovávání[202]. Po provedené likvidaci již osobní údaje nebudou nadále existovat a správce přestává být za jejich zpracování odpovědný, neboť již správcem nadále nebude[203].

Způsob likvidace závisí zejména na nosiči, na němž jsou osobní údaje zachyceny a uchovávány – zejména zda se jedná o papírové či elektronické dokumenty. V každém případě však musí správce zabezpečit, aby jím provedená likvidace byla nevratná. Ačkoliv jsou si v dnešní době již zaměstnavatelé v postavení správců svých povinností ve vztahu k likvidaci nepotřebných či neaktuálních údajů většinou vědomi, obzvláště v případě elektronických souborů dochází k jejich neodbornému vymazání, kdy jednou vymazané soubory je později možné z paměti obnovit. Za likvidaci totiž není možné považovat takový způsob „zničení" dat, která by bylo v budoucnosti možné stejnými nebo jinými technickými prostředky obnovit tak, aby znovu nabyla charakteru osobních údajů. Bezpečnou likvidací je v takovém případě nutné rozumět nejen pouhé vymazání

[201] Viz též dokument sub. pozn. č. 199.
[202] Srov. důvodová zpráva k zákonu č. 101/2000 Sb., sněmovní tisk č. 374/0, dostupná z http://www.psp.cz/sqw/text/tiskt.sqw?O=3&CT=374&CT1=0.
[203] Kučerová, A. Bartík, V. Peca, J. Neuwirt, K., Nejedlý, J. *Zákon o ochraně osobních údajů. Komentář.* 1. vyd. Praha: C. H. Beck, 2003, s. 154.

údajů z jejich nosiče, nýbrž také přepsání původního souboru jakýmikoliv jinými daty (včetně prázdných znaků)[204]. Netřeba dodávat, že u papírových dokumentů je odpovídajícím způsobem zejména jejich skartace, nikoliv pouhé vyhození mezi odpad, neboť tak samozřejmě není splněna povinnost správce zabránit možnému zneužití těchto údajů, která platí i po skončení jejich zpracování[205]. Zaměstnavatel v pozici správce může likvidací pověřit zpracovatele, což bude obvyklé zejména v případě delší spolupráce se zpracovatelem, přičemž záruka zabezpečení likvidace je již obsaženo ve smlouvě o zpracování osobních údajů, kterou mezi sebou zaměstnavatel a jím pověřený zpracovatel uzavřeli v souladu s § 6 Zákona již na počátku vzájemné spolupráce.

Základním a nejčastějším důvodem pro likvidaci osobních údajů je skutečnost, že pomine účel, pro který byly údaje zpracovávány. V případě, že tato skutečnost nastane, stanoví Zákon v ust. § 20 odst. 1 povinnost odpovědné osoby likvidaci provést[206]. Lze však zcela jistě doporučit, aby před likvidací dokumentů byly po dobu běhu obecné promlčecí lhůty (tj. tříleté promlčecí doby dle ustanovení § 101 ObčZ) archivovány ty dokumenty, z nichž vyplývají nebo by případně mohly vyplynout jakékoliv nároky zaměstnance vůči zaměstnavateli (např. evidence pracovní doby, dovolené nebo dohoda o odpovědnosti za schodek na svěřených hodnotách, které je zaměstnanec povinen vyúčtovat)[207].

Je však pravdou, že Úřad opakovaně upozorňuje na překračování doby zpracování (a to zejména ve formě uchovávání údajů) nezbytné k dosažení účelu zpracování[208]; není zejména přípustné uchovávat veškeré kontaktní údaje bývalého zaměstnance (včetně telefonního čísla) po ukončení pracovního poměru či v osobním spise archivovat i vyhodnocené testy, jimž se zaměstnanec podrobil v průběhu přijímacího řízení, neboť se zpracování jejich výsledků zaměstnanec souhlasil výhradně pro účely tohoto přijímacího řízení. Po vzniku pracovního

[204][204] Dokument sub. pozn. č. 202.
[205] § 13 odst. 1 ZOOÚ
[206] Bartík, V., Janečková, E. Likvidace osobních údajů jako součást zpracování. *Právní rádce*. 2010, č. 2, s. 34.
[207] K tomu více viz subkapitola 3.2 zabývající se uchováváním osobních údajů.

poměru tak již tyto testy logicky svému účelu nadále nemohou sloužit a jejich další zpracovávání proto není dovolené.

S likvidací souvisí také blokování údajů (§ 4 písm. h) Zákona). Na rozdíl od likvidace však při blokování osobních údajů nedochází k jejich trvalému zničení, nýbrž pouze dočasnému znepřístupnění. Údaje tedy i nadále existují, nemohou být však v daném okamžiku zpracovávány. Pro zaměstnavatele je důležité být si vědom případů, kdy mu jako správci vzniká ze Zákona povinnost osobní údaje svých zaměstnanců blokovat[209]. První z nich nastává v situaci, kdy správce zjistí nepřesnost jím zpracovávaných údajů[210]. Správce je pak povinen údaje blokovat, dokud nebudou opraveny, jinak musí přistoupit k jejich likvidaci, neboť není oprávněn zpracovávat nepřesné a neaktuální údaje. S touto povinností správce pak souvisí právo subjektu údajů blokování údajů po správci požadovat, jestliže se domnívá, že správce zpracovává jeho údaje v rozporu se Zákonem[211]. Posledním případem, kdy Zákon ukládá blokaci (a rovněž také i likvidaci) údajů, je tehdy, byla-li správci uložena likvidace údajů jako jedno z opatření k nápravě[212]. Správce má možnost proti takovému rozhodnutí podat námitku k předsedovi Úřadu, přičemž do rozhodnutí o námitce musí být údaje blokovány[213].

[208] Viz Výroční zpráva ÚOOÚ za rok 2009, s. 12.
[209] K pojmu blokování více viz kapitola 3.
[210] § 5 odst. 1 písm. c) ZOOÚ
[211] § 21 odst. 1 ZOOÚ
[212] Srov. dokument sub. pozn. č. 206, s. 35.
[213] § 40 odst. 2 ZOOÚ

7. Vybrané problematiky

V této kapitole bych se chtěla věnovat vybraným problémům, které v současnosti patří v oblasti ochrany osobních údajů v pracovněprávních vztazích k těm nejaktuálnějším. Jsem si vědoma skutečnosti, že na některé otázky existuje mezi odbornou veřejností více odlišných názorů; i z toho důvodu však považuji za žádoucí nalezení určitého kompromisu mezi oprávněnými zájmy zaměstnavatelů a vyžadováním náležité úrovně ochrany osobních údajů ze strany orgánů státní správy (ÚOOÚ, inspekce práce), potažmo soudů. Zatímco u některých problematik nečiní zaměstnavatelům potíže podřídit se platné právní úpravě a jejímu ustálenému výkladu, u dalších otázek, obzvláště těch spojených s kontrolou trávení pracovní doby zaměstnanců a nakládání s prostředky zaměstnavatele, dosud vzájemného konsenzu všech zúčastněných stran dosaženo nebylo. Je proto namístě se jimi i po několikáté zabývat a i nadále se pokoušet nalézt rovnováhu mezi omezením práv jedněch při oprávněném prosazování práv druhých, jako se o to v podstatě pokouší celé odvětví právní úpravy ochrany osobních údajů.

7.1 Monitoring zaměstnanců

Zatímco vývoj informačních a komunikačních technologií, jakož i sledovacích zařízení (umožňujících jak otevřené, tak skryté sledování), učinil za poslední dvě desetiletí nepředstavitelný pokrok, právní úprava ochrany soukromí za tímto technologickým rozvojem notně zaostává[214]. Možnosti monitoringu zaměstnanců na pracovišti přitom souvisí zejména s dostupností technických prostředků, které jednotlivé způsoby sledování umožňují. S rozvojem moderních technologií a současně snižováním jejich pořizovací ceny přitom roste subjektivní potřeba zaměstnavatelů své zaměstnance při jejich pohybu na pracovišti[215] sledovat

[214] Bartík, V., Janečková, E. *Ochrana osobních údajů v aplikační praxi.* 2. vyd. Praha: Linde, 2010, s. 139.

[215] Zákoník práce pojem „pracoviště“ nikterak nedefinuje. Za pracoviště je tak možné považovat jak přímo pracovní místo (tj. např. stůl a židle / prodejní pult / místo u výrobní linky), tak i širší okolí, v němž se zaměstnanec během své pracovní doby pohybuje (např. zázemí prodejny, zasedací místnosti apod.).

a kontrolovat, zda čas tam strávený skutečně věnují plnění pracovních úkolů. Narušování soukromí jednotlivce a jeho práva na důstojné zacházení, zachování listovního tajemství a dalších základních práv je v důsledku toho mnohem jednodušší než před několika desítkami let, a proto je více než kdy dříve žádoucí dbát důsledně o to, aby ke sledování zaměstnanců docházelo pouze v těch případech, kdy vlastní zájem zaměstnavatele značně převyšuje zájem společnosti na plném zachovávání těchto práv. I přesto však nesmí být na základě principu proporcionality[216] do ústavně zaručených práv zasahováno více, než je nezbytné, neboť zaměstnanci mají i na pracovišti právo na určitou míru soukromí a na to, aby si v nezbytném rozsahu mohli na pracovišti vyřídit své soukromé záležitosti[217]. Pakliže nejsou ze strany zaměstnavatele informováni o zvláštním způsobu sledování jejich aktivit na pracovišti, mohou oprávněně očekávat důvěrnost zpráv a telefonických hovorů vyřizovaných na pracovišti[218]; toto však zaměstnance samozřejmě neopravňuje k zařizování soukromých záležitostí během pracovní doby v rozsahu větším, než je nezbytně nutné.

Toto oprávnění zaměstnanců pak určuje hranice pro možnost kontroly pošty zaměstnanců (v papírové i elektronické podobě), jejich telefonních hovorů ve firemních prostorách či dokonce kamerového sledování během pracovní doby. Na druhé straně, limitem pro soukromí zaměstnanců je právo zaměstnavatele na efektivní plnění jím zadaných pracovních úkolů a také jeho práva na ochranu svého majetku[219] (tj. zejména zabránění, aby zaměstnanci využívali pracovní prostředky zaměstnavatele k osobním potřebám, neboť ty jsou ve vlastnictví zaměstnavatele a pouze on také určuje možnost jejich využití[220]). Je proto úkolem zaměstnavatele, aby v mezích zákona určil jasná pravidla pro nakládání

[216] Stanovisko ÚOOÚ č. 2/2009 – Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště.
[217] Dokument sub. pozn. č. 214, s. 146.
[218] Srov. rozsudek Evropského soudu pro lidská práva ve věci Copland proti Spojenému království ze dne 3.4.2007.
[219] Bartík, V., Janečková, E. Ochrana soukromí na pracovišti – e-mailová pošta. *Práce a mzda.* 2009, č. 11, s. 28.
[220] Morávek, J. *Ochrana osobních údajů v pracovněprávní agendě.* 1. vyd. Praha: BMSS Start, 2010, s. 12.

s pracovními prostředky, které zaměstnancům k výkonu jejich práce propůjčí, a rovněž stanovil, jakým způsobem bude nakládání s nimi kontrolováno.

Za tímto účelem mu zákoník práce v ustanovení § 316 odst. 1 výslovně umožňuje přiměřeně kontrolovat, zda zaměstnanci nevyužívají bez jeho souhlasu výrobní a pracovní prostředky za jiným účelem než plnění pracovních úkolů, když zároveň zaměstnancům zakazuje užívat pracovní prostředky zaměstnavatele (včetně výpočetní techniky a telekomunikačních zařízení) pro svou osobní potřebu. Ve vztahu ke kolizi tohoto oprávnění s ochranou soukromí[221] pak dále zákoník práce stanoví, že tam, kde to odůvodňuje zvláštní povaha činnosti zaměstnavatele, je zaměstnavatel při dodržení dalších podmínek oprávněn v určité míře narušovat soukromí zaměstnanců na pracovišti tím, že je vystaví sledování (kamerový systém na pracovišti), odposlechu a záznamu telefonických hovorů či kontrole elektronické i listovní pošty (§ 316 odst. 2 ZP). V takovém případě je však povinen zaměstnance přímo informovat o rozsahu takové kontroly a způsobu jejího provádění (§ 316 odst. 3 ZP).

Pakliže tedy není podmínka zvláštní povahy činnosti zaměstnavatele splněna, není zaměstnavatel oprávněn podrobovat své zaměstnance sledování, a to ani kdyby k tomu dal zaměstnanec souhlas[222]. Ústavně zaručená práva a svobody, jakými je i právo každého na ochranu soukromí, soukromého a rodinného života a zachování listovního a obdobného tajemství, jsou totiž nezadatelná a nezcizitelná[223]. Jedinec se jich sám od sebe nemůže vzdát a jejich narušení je možné pouze ve výjimečných případech[224], stanoví-li tak v souladu s ústavním pořádkem zákon[225] (tj. například ustanovení § 316 odst. 2 ZP). Vedle toho by navíc takový úkon, jímž by se zaměstnanec vzdal předem svých práv, byl podle

[221] Dokument sub. pozn. č. 214, s. 141.
[222] Ke stejnému závěru dospěla i Pracovní skupina 29; souhlas subjektu tak nezbavuje správce povinnosti zpracovávat osobní údaje zaměstnanců (včetně jejich monitoringu) v souladu s právními předpisy a pouze v nezbytném rozsahu. Srov. Stanovisko WP 48 o zpracování osobních údajů v souvislosti se zaměstnáváním, s. 18.
[223] Čl. 1 LZPS
[224] Dokument sub. pozn. č. 214, s. 142.
[225] Viz také nálezy Ústavního soudu sp.zn. IV. ÚS 554/03 nebo I. ÚS 452/09.

ustanovení § 19 písm. c) zákoníku práce absolutně neplatný, a nadto je ustanovení § 316 ZP ustanovením kogentním[226]. Způsob sledování, je-li přípustný, proto musí být omezen do té míry, aby byla šetřena osobnost zaměstnance a jeho soukromí. Velice trefně je tento princip vyjádřen ve Stanovisku WP 48[227]: právo zaměstnavatele zpracovávat osobní údaje zaměstnanců v případě ochrany jeho oprávněného zájmu nedává zaměstnavatelům blanketní šek ke zpracování osobních údajů zaměstnanců v libovolném rozsahu.

Za činnosti zvláštní povahy, při jejichž výkonu je zaměstnavatel oprávněn podrobit své zaměstnance sledování, jsou přitom považovány zejména takové činnosti, kde je třeba dbát zvýšeného nároku na chování zaměstnanců (např. vzhledem k manipulaci s vyššími majetkovými hodnotami, ochraně obchodního tajemství či know-how zaměstnavatele nebo kupříkladu při nakládání s testy státních maturit)[228]. Paušální seznam činností, při nichž je monitoring povolen, neexistuje a vzhledem k rozmanitosti vykonávaných činností ani existovat nemůže. Parametry (např. četnost a způsob) sledování by měl zaměstnavatel nastavit podle „závažnosti“ důvodu ke sledování (např. ochrana majetku v porovnání s ochranou zdraví). Na maximální míru musí být v tomto směru omezen způsob sledování pracovní výkonnosti zaměstnanců[229].

Problematikou různých způsobů sledování zaměstnanců na pracovišti se také dlouhodobě zabývá Rada Evropy[230] a samozřejmě také Evropská unie. Úřad Evropského inspektora ochrany údajů vydal v roce 2010 směrnici[231] vztahující se k problematice kamerového sledování, nicméně její závěry lze vztáhnout na celou oblast monitoringu zaměstnance. Úřad Evropského inspektora v této směrnici ve

[226] Stanovisko ÚOOÚ č. 2/2009 – Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště. Srov. též ustanovení § 4b odst. 1 ZP.
[227] Stanovisko WP 48 o zpracování osobních údajů v souvislosti se zaměstnáváním, s. 20.
[228] Dokument sub. pozn. č. 214, s. 142.
[229] Bělina, M. a kol. *Zákoník práce. Komentář*. 2. vyd. Praha: C.H. Beck, 2010, s. 818.
[230] Viz např. rozsudek Evropského soudu pro lidská práva ve věci Niemietz proti Německu, zmiňovaný v kapitole 6, nebo rezoluce č. 1604 (2008) ze dne 25.01.2008, dostupná z http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta08/ERES1604.htm.

vztahu k zaměstnancům zmiňuje zejména kontraproduktivnost excesivního monitoringu, kdy vědomí neustálého sledování vystavuje zaměstnance stresu a přínos monitoringu ke zlepšení pracovních výsledků je tak značně oslaben. Přehnané sledování a zasahování do soukromí zaměstnanců také může významně narušit důvěru zaměstnanců v organizaci zaměstnavatele a tím snížit i jejich zájem na jejím efektivním fungování. Evropský inspektor proto zdůrazňuje, že sledování zaměstnanců nelze nikdy ospravedlnit pouze požadavkem kontroly výkonnosti a kvality práce zaměstnanců, kontroly dodržování vnitřních předpisů nebo požadavkem získání důkazního materiálu pro případ sporu se zaměstnancem vzniklého z pracovněprávního vztahu.

7.1.1 Kamerové systémy na pracovišti

Kamerové systémy jako jeden z prostředků sledování zaměstnanců můžeme v podstatě rozdělit na dva typy: jednak se může jednat o kamerové systémy, které pouze monitorují momentální dění, aniž by při něm docházelo k pořizování záznamu, a jednak systémy, u nichž dochází k ukládání záznamu na datový nosič. Na základě tohoto dělení je pak možné rozhodnout, zda provozování kamerového systému bude podléhat působnosti Zákona či nikoli, neboť vždy, když je kamerový systém určený ke sledování osob vybaven záznamovým zařízením, dochází k systematickému shromažďování snímků a tím i zpracování osobních údajů osob na něm zachycených[232].

Provozování kamerového systému bez pořizování záznamu však není zpracováním osobních údajů ve smyslu ZOOÚ. I v takovém případě je však provozovatel kamerového systému povinen respektovat Listinu základních práv a svobod, garantující právo na respektování soukromého života, a ustanovení občanského zákoníku týkající se ochrany osobnosti. Rovněž při instalaci tohoto typu kamerového systému je proto nutné dodržet základní zásady: především není

[231] EDPS Video-Surveillance Guidelines, dostupné z http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf.
[232] Výroční zpráva ÚOOÚ za rok 2008, s. 42.

přípustné, aby byl systém instalován v prostorách, které slouží ryze soukromým účelům, jako jsou např. toalety, sprchy či šatny, ale také ani v individuálních kancelářích a odpočinkových místnostech[233]. V ostatních prostorách by potom mělo být vyznačeno, že se jedná o prostory monitorované kamerovým systémem. Nejedná-li se o monitorování na základě zákona, jež je možné provozovat i bez souhlasu subjektů, měly by ke svému kamerovému sledování dát monitorované osoby v souladu s § 12 odst. 3 ObčZ souhlas[234]. Při instalaci systému je rovněž nutné mít na paměti, že i přes absenci pořizování záznamu může dojít ke zneužití těchto údajů (např. pokud by se třetí osoba připojila přes vzdálený přístup na monitorovací okruh či pokud by osoba obsluhující kamery neoprávněně pořídila záznam z kamer[235]), a v souladu s tímto zajistit dostatečnou bezpečnost přenosu mezi kamerami a monitorovací centrálou.

Na rozdíl od „prostého“ kamerového sledování bez pořizování záznamu je za zpracování osobních údajů ve smyslu Zákona naopak považováno provozování kamerového systému, pokud je vedle kamerového sledování prováděn rovněž záznam pořizovaných záběrů nebo jsou v záznamovém zařízení uchovávány informace za účelem jejich využití k identifikaci osob v souvislosti s určitým jednáním. Vzhledem k uchovávání záznamu je totiž možné presumovat, že se získané záběry budou později dále zpracovávat, neboť v opačném případě by jejich pořizování ztrácelo smysl[236]. Ani toto provozování kamerového systému však nemusí ZOOÚ podléhat vždy; bude tomu tak pouze v případech, kdy je možné na základě pořízeného záznamu přímo či nepřímo fyzickou osobu identifikovat (tj. pokud budou ze snímku, na němž bude zachycena, patrné její charakteristické rozpoznávací znaky, zejména obličej[237]). Pokud nebude možné fyzickou osobu zachycenou na záznamu bez použití dalších doprovodných údajů ztotožnit, nebude se jednat o osobní údaj ve smyslu ustanovení § 4 písm. a) ZOOÚ. Jelikož však na

[233] Srov. dokument sub. pozn. č. 231, s. 29.
[234] Matoušová, M. a kol. *Ochrana osobních údajů v otázkách a odpovědích*. 1. vyd. Praha: ASPI Publishing, 2004, s. 83.
[235] Srov. dokument sub. pozn. č. 231, s. 9.
[236] Srov. Výroční zpráva ÚOOÚ za rok 2008, s. 42.

záznamu budou zachyceny tváře jednotlivých osob, je nutné se záznamem nakládat alespoň jako s potenciálním osobním údajem, neboť není samozřejmě vyloučeno, že k identifikaci osob na záznamu dojde později[238]. A protože taková identifikace je do určité míry pravděpodobná, obsah záznamu se v budoucnosti může stát osobním údajem a jeho pořizování tak ZOOÚ podléhat bude. Proto je nutné veškeré informace, které budou o konkrétních osobách tímto způsobem zaznamenány a umožňují jejich přímou nebo i nepřímou identifikaci, považovat za osobní údaje ve smyslu Zákona[239].

Zákon se také na provoz kamerového systému se záznamem bude vztahovat jen tehdy, dá-li se předpokládat, že se na záznamu budou objevovat fyzické osoby. Zákonu tak nebude podléhat například sledovací zařízení zaměřené výhradně na cenný exponát v muzeu (sledující jeho stav, vlhkost vzduchu a další parametry významné pro péči a zachování stavu exponátu), pokud je snímaný rozsah tak malý, že lze vyloučit zachycení osob pohybujících se v okolí exponátu, respektive pokud by se na záznamu fyzické osoby objevovaly velice zřídka a pouze náhodně[240].

Údaje získané prostřednictvím záznamu, jejichž pořizování podléhá Zákonu, lze potom zpracovávat (a tedy i kamerový systém vůbec provozovat) v následujících případech[241]:

a) je-li to nezbytné k plnění úkolů uložených zákonem (např. zákon o Policii České republiky),

b) se souhlasem subjektu údajů (tento požadavek je často v praxi obtížně realizovatelný, neboť nelze předem určit okruh osob, které se budou v dosahu kamer nacházet[242]),

---

[237] Bartík, V., Janečková, E. Kamery se záznamovým zařízením na pracovišti. *Práce a mzda.* 2010, č. 3, s. 30.
[238] Srov. dokument sub. pozn. č. 214, s. 145.
[239] Z rozhodovací činnosti ÚOOÚ – K provozování kamerového systému na pracovišti (čj. 42/06/SŘ).
[240] Srov. dokument sub. pozn. č. 234, s. 61, jakož i Výroční zpráva ÚOOÚ za rok 2008, s. 46.

c) bez souhlasu subjektů údajů za využití ustanovení § 5 odst. 2 písm. e) ZOOÚ, tj. je-li to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo dotčené osoby (vzhledem k použití slova „nezbytné“ tedy musí být předem vyčerpány veškeré méně invazivní možnosti, jimiž mohlo být požadovaného účelu taktéž dosaženo[243]). Ani v tomto případě nesmí být samozřejmě monitorování v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života.

Dalšími pravidly pro používání kamerového systému se záznamem jsou v souladu se zásadami a povinnostmi při shromažďování a dalším zpracovávání osobních údajů také[244]:

– zákaz nadměrného zasahování do soukromí

Při úvaze o použití kamerového systému na pracovišti by měl zaměstnavatel především zvážit právě dopady sledování do soukromí zaměstnanců a zhodnotit, zda skutečně přínos kamer převáží nad narušením jejich osobního života. Jak již bylo uvedeno výše, kamerový systém lze použít pouze tehdy, jestliže sledovaného účelu nelze účinně dosáhnout jinými, méně invazivními prostředky (např. při ochraně majetku uzamčením prostoru – jestliže nebude na dveřích skladu zámek, ani kamerový systém majetek v něm uložený neochrání). Není rovněž přípustné instalovat kamery v prostorách sloužících výlučně k úkonům osobní povahy (již výše zmiňované toalety, převlékárny apod.). Jak uvádí Úřad ve své Výroční zprávě za rok 2008[245], nejzávažnějším nedostatkem v oznámeních o registraci zpracování osobních údajů s využitím kamerového systému je zejména nesprávné posouzení poměru mezi hodnotami, které mají být kamerovým systémem chráněny, a hodnotami, do kterých kamerový systém zasahuje. Dodržování tohoto pravidla lze

---

[241] www.uoou.cz / Na aktuální téma / Komentář k Zásadám provozování kamerového systému z hlediska zákona o ochraně osobních údajů
[242] Dokument sub. pozn. č. 237, s. 31.
[243] S tímto názorem však někteří autoři polemizují a při splnění všech ostatních podmínek považují provozování kamerového systému za přípustné i tehdy, jde-li sledovaného účelu dosáhnout i jinými prostředky (srov. dokument sub. pozn. č. 237, s. 33). Názor Úřadu je nicméně totožný i s postojem Evropského inspektora ochrany údajů (srov. dokument sub. pozn. č. 231, s. 19).
[244] Srov. dokument sub. pozn. č. 234.

zajistit již při plánování kamerového systému nastavením jeho parametrů – kamery by měly být v odpovídajícím počtu rozmístěny pouze tak, aby skutečně zaznamenávaly dění výhradně ve vymezeném prostoru a aby jejich rozlišení nebylo větší, než je pro daný účel potřebné[246]. V souladu s posouzením převažujících hodnot tak není kupříkladu možné umístit kameru do kuchyňky sloužící k občerstvování zaměstnanců s odůvodněním, že tak bude zjištěna identifikace osoba, která si ráda přivlastňuje svačiny druhých uchovávané ve společné lednici[247].

– specifikace sledovaného účelu

Vždy je třeba zcela jednoznačně stanovit účel pořizování záznamů, přičemž tento účel musí korespondovat s právem chráněnými zájmy správce (např. ochrana majetku před krádeží). Záznamy pak mohou být využity pouze v souvislosti se zjištěním události, která tyto zájmy správce poškozuje; přípustné je jedině také další využití ve veřejném zájmu (např. pro účely vyšetřování trestného činu). Není rozhodně možné, aby byly záznamy využity i k jinému účelu, než který byl původně stanoven[248].

– časově omezené uchovávání záznamu

V souladu s ustanovením § 20 odst. 1 ZOOÚ by doba uchovávání záznamu neměla překročit dobu, která je nutná pro naplnění účelu, kvůli němuž byl záznam pořizován. Podle názoru Úřadu by data měla být uchovávána nejdéle několik dnů (dle mého názoru lze za přiměřenou dobu považovat 3 až 5 pracovních dnů včetně dne pořízení záznamu; obecně Úřad za přiměřenou považuje dobu 3 kalendářních

---

[245] Výroční zpráva ÚOOÚ za rok 2008, s. 43.
[246] Dokument sub. pozn. č. 237, s. 31. I s ohledem na ušetření nákladů by zavedení kamerového systému měl u zaměstnavatele předcházet bezpečnostní audit, jenž by posoudil jednak vůbec přípustnost kamerového sledování a jednak navrhl nejvhodnější technické řešení, které zaměstnavateli umožní dosáhnout zamýšleného účelu při maximálním zachování práv zaměstnanců.
[247] Srov. dokument sub. pozn. č. 231, s. 20.
[248] Jedná se o problematiku tzv. *function creep*, tedy odchýlení se od původního účelu. V oblasti pracovněprávních vztahů přichází nejčastěji v úvahu využití záznamu jako důkazního materiálu v disciplinárním řízení se zaměstnancem.

dnů[249], Evropský inspektor pro ochranu osobních údajů připouští jeden týden za předpokladu, že lze vyloučit výskyt náhodných osob[250] na záznamu) a po uplynutí této doby vymazána. V odůvodněných situací lze však připustit i delší uchovávání záznamu (jedná-li se kupříkladu o zaznamenávací zařízení na obtížněji dostupném místě). Pouze však dojde-li ke konkrétní bezpečnostní události, měla by být data zpřístupněna orgánům činným v trestním řízení či jinému oprávněnému subjektu[251]. Nejspolehlivějším zajištěním, že doba uchování záznamu nepřekročí maximální hranici, je pak nastavení automatického smazání záznamu po uplynutí určité doby.

– zajištění ochrany záznamu

Dále je třeba také zajistit dostatečnou ochranu záznamů před neoprávněným nebo nahodilým přístupem a dalším neoprávněným zpracováním. Uplatní se zde přitom stejná pravidla jako při zajišťování bezpečnosti jakýchkoli jiných zpracovávaných osobních údajů.

– informace subjektu údajů

Subjekt údajů musí být o použití kamerového systému samozřejmě vhodně informován, obvykle se tak děje formou nápisu v monitorovaném prostoru. Tato prvotní informace o monitorování prostoru však musí kromě informace o skutečnosti, že je prostor monitorován, obsahovat alespoň údaj o tom, kde se subjekt údajů může o prováděném monitoringu dozvědět více podrobností[252].

– notifikace ÚOOÚ

Dle ustanovení § 16 ZOOÚ je správce navíc povinen oznámit úmysl zahájit provoz kamerového systému ÚOOÚ, a to ještě před jeho spuštěním (o oznamovací

[249] Ke lhůtě tří pracovních dnů se však ÚOOÚ přiklonil ve svém Informačním bulletinu č. 2/2011, s. 5.
[250] Tzv. *passers-by*. Jestliže se náhodné osoby mohou na záznamu objevit, doporučuje Evropský inspektor data uchovávat maximálně 48 hodin.
[251] Viz Stanovisko ÚOOÚ č. 1/2006 – Provozování kamerového systému z hlediska zákona o ochraně osobních údajů.
[252] Srov. dokument sub. pozn. č. 237, s. 31.

povinnosti bylo podrobně pojednáno v subkapitole 5.4). Registrační formulář pak obsahuje zvláštní část věnovanou právě zpracování osobních údajů prostřednictvím kamerového systému.

Nejčastějším důvodem, jenž vede zaměstnavatele k využití kamerového systému na pracovištích, bývá ochrana majetku a prevence majetkových trestných činů a v některých případech také kontrola dodržování bezpečnosti ochrany zdraví při práci či důležitých technologických postupů. Zaměstnavatelé přikračují k instalaci kamer v rozličných prostorách svých podniků; kamery tak nalezneme ve skladech, výrobních halách, bankovních či úředních přepážek, ale také na recepcích či přímo v kancelářích[253]. Použití monitorovací systému na pracovišti je však podmíněno splněním zákonných podmínek, které vychází zejména z ustanovení § 316 odst. 2 ZP, což znamená, že využití kamer je zapovězeno tam, kde není dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele. Jak však již bylo uvedeno výše, pojem „závažný důvod spočívajícího ve zvláštní povaze činnosti“ je poměrně vágní, a dosud nebyl nikterak rozveden ani soudní judikaturou. Vždy tak bude záležet na posouzení konkrétního zaměstnavatele, zda použití kamer nebo i jiného sledovacího zařízení shledá ve svém případě jako odůvodněné. Dle názoru Úřadu lze o využití kamer uvažovat zejména v prostředí, v němž jsou kladeny zvýšené nároky na chování zaměstnanců (tj. například činnost peněžních ústavů nebo pracoviště, na nichž zaměstnanci přicházejí do styku s informacemi podléhajícími určitému stupni utajení). Za žádných okolností však není využití kamer odůvodněné pouhým zájmem zaměstnavatele kontrolovat své zaměstnance či kvalitu jejich práce bez dalšího závažného důvodu[254].

Jako další se stejně jako v ostatních případech monitoringu zaměstnanců nabízí otázka, zda je možné k němu přistoupit i bez souhlasu dotčených osob. Za předpokladu, že jsou splněny výše uvedené podmínky a je naplněno ustanovení § 316 odst. 2 ZP, je většinou možné na provoz kamerového systému aplikovat

[253] Srov. Výroční zpráva ÚOOÚ za rok 2007, s. 64.

zákonnou výjimku podle ustanovení § 5 odst. 2 písm. e) Zákona, neboť v takovém případě je zpracování osobních údajů subjektů nezbytné pro ochranu práv a chráněných zájmů zaměstnavatele.

S ohledem na informační povinnost zaměstnavatele provozujícího kamerový systém je vhodné, aby byla pravidla jeho užívání stanovena ve vnitřním předpise, případně i vícero vnitřních předpisech u zaměstnavatelů, u nichž se nedá vyloučit, že na kamerovém záznamu budou zachyceny i třetí osoby kromě zaměstnanců. Obsahem takového předpisu by mělo být zejména přesné vymezení a specifikace účelu provozování kamer, určení sledovaného prostoru a rozmístění kamer, stanovení způsobu pořizování záznamů, určení způsobu jejich využití a nakládání s nimi, určení nezbytně nutné doby k uchovávání záznamů, vymezení pravomoci a odpovědnosti pracovníků provádějících obsluhu zařízení a manipulujících se záznamy, a to včetně stanovení způsobu a četnosti školení odpovědných pracovníků a jejich zastupitelnost. Vnitřní předpis může také upravovat formalizované disciplinární řízení se zaměstnanci, kteří porušili nebo nedodrželi předepsané bezpečnostní postupy. S tímto vnitřním předpisem by měli být všichni zaměstnanci prokazatelně seznámeni.

Zaměstnavatelé by si také měli být vědomi skutečnosti, že kamery často nebudou zaznamenávat pouze zaměstnance, nýbrž i další osoby, které se na pracovišti vyskytnou (zákazníci, obchodní návštěvy apod.). I vůči nim je tak nutné splnit informační povinnost, tj. zajistit, aby tyto osoby byly informovány o tom, že je prostor monitorován, kdo kamerový systém provozuje a kde lze případně získat další informace (obsažené ve směrnici či obdobném dokumentu zaměstnavatele). Ohledně požadavku vymezení rozsahu zpracovávaných údajů při splnění primární informační povinnosti je u kamerového systému myslitelná jistá benevolence, neboť u něj prakticky nelze dopředu vymezit, kolik osob a v jakých situacích tento systém zaznamená. Rozsah údajů se také může značně lišit v závislosti na umístění

[254] Srov. dokument sub. pozn. č. 214, s. 54-55.

jednotlivých kamer. Proto postačuje, je-li součástí informační povinnosti odkaz, kde lze v případě zájmů získat více informací[255].

Ačkoliv by tak při postupném použití těchto vodítek i výše uvedených pravidel mělo být v zásadě jednoduché učinit rozhodnutí o využívání kamerového systému na pracovišti, zůstává přesto tato otázka pro mnoho zaměstnavatelů nejasná. I vzhledem k rychlému rozvoji monitorovacích zařízení a zvýšením jejich cenové dostupnosti se tak dá očekávat vznik nových, dosud Zákonem ani odbornou veřejností neřešených otázek a šedých zón v souvislosti s užíváním kamerových systémů (a jejich rostoucí oblibou).

Nejčastější chyby zaměstnavatelů v souvislosti s používáním kamerového systému lze proto vyvodit mimo jiné i z rozhodovací praxe Úřadu. Velice často bývají kamery využívány pouze preventivně, aniž by představovaly nezbytný prostředek k naplnění deklarovaného účelu, a jejich využití tak neodůvodňuje zásah do práv zaměstnanců, který jeho využití způsobí. Míru tohoto zásahu je však možné účelu přizpůsobit; ne vždy je nezbytné, aby byly monitorovány všechny obchodní prostory, aby se tak dělo po celou provozní dobu či aby kamery měly vysoké rozlišovací schopnosti[256] (stěží si lze představit oprávněný zájem zaměstnavatele vyžadující nasazení kamer s rozlišením umožňující kupříkladu přečtení textu na displeji mobilního telefonu zaměstnance). Při stanovení kritérií pro posouzení, nakolik je zájem zaměstnavatele na využití kamerového systému odůvodněný, je možné vyjít také z nálezu Ústavního soudu sp.zn. Pl. ÚS 4/94, jenž řeší případ kolize vícera základních lidských práv a posouzení jejich „váhy“ v dané situaci[257]. Je proto nutné posoudit, nakolik je využití kamerového systému potřebné (tj. zda nelze stejného účelu dosáhnout i jinými, méně invazivními

[255] Podle doporučení evropského inspektora ochrany údajů (srov. dokument sub. pozn. č. 231, s. 64) bude jako prvotní informace o kamerovém sledování postačující následující sdělení: „Z důvodu Vaší bezpečnosti je tato budova a její nejbližší okolí monitorováno kamerovým systémem. Záznam je uchováván po dobu 72 hodin. Bližší informace naleznete na www.nasedomena.cz nebo na telefonním čísle +420 111 222 333.“
[256] Výroční zpráva ÚOOÚ za rok 2007, s. 12.
[257] Srov. dokument sub. pozn. č. 237, s. 31.

prostředky) a zda je pro daný případ vůbec vhodné (tj. zda se jeho využitím skutečně deklarovaného účelu dosáhne)[258].

V jedné z výročních zpráv ÚOOÚ[259] lze také najít odstrašující, nicméně bohužel jistě ne ojedinělý případ, kdy zaměstnavatel na svém pracovišti provozoval kamerový systém, přičemž jeho využití odůvodnil ochranou majetku, prevencí krádežím a také zdraví vlastních zaměstnanců. Při kontrole ze strany Úřadu však vyšlo najevo, že kamery sledovaly především zaměstnance a záznamy byly vyhodnocovány pro posouzení jejich pracovní výkonnosti; tyto výsledky byly dokonce využívány k šikanování některých zaměstnanců. Deklarovaného účelu ochrany majetku zcela jistě nebylo prostřednictvím kamerového systému možné dosáhnout, neboť kamery byly spuštěné pouze během pracovní doby, a naopak po dobu, kdy byl prostor opuštěn, nebyly kamery v provozu. Kontrolovaná společnost navíc ani nedisponovala souhlasem zaměstnanců s monitorováním. I kdyby ho však měla k dispozici, nebylo by ho možné vzít na zřetel, neboť kamery byly provozovány v rozporu s účelem, pro nějž byl souhlas poskytnut.

Ze strany Úřadu byla také odmítnuta (resp. nepovolena) registrace zpracování osobních údajů prostřednictvím provozování kamerového systému v jednom z obchodních řetězců, kde měl být sledován prostor každé pokladny, a to s ohledem na ustanovení § 5 odst. 2 písm. e) a § 10 Zákona, a také § 316 odst. 2 zákoníku práce. Předseda Úřadu ve svém rozhodnutí odkázal na pojem soukromí, který v České republice zatím bývá vykládán příliš úzce, přičemž s ohledem na význam tohoto základního práva je nezbytný výklad extenzivní. Ochrana poskytovaná zaměstnancům prostřednictvím Zákona a zákoníku práce přitom směřuje k naplnění těch ústavně garantovaných práv, jež souvisí s lidskou důstojnosti a ochranou soukromého a rodinného života. Vzhledem k důležitosti a nezcizitelnosti těchto práv tak nelze pojem soukromí na pracovišti omezovat pouze na úzkou oblast důvěrné sféry osobního života zaměstnance, neboť zahrnuje celou škálu situací, kdy zaměstnanec oprávněné očekává zvýšenou ochranu své osobní

[258] Srov. Výroční zpráva ÚOOÚ za rok 2008, s. 43.

integrity. Podrobením zaměstnance soustavnému sledování jeho chování (k čemuž by došlo v důsledku celodenního zaměření kamer na pokladnu) podle Úřadu právě k takovému nepřípustnému zásahu do soukromí zaměstnance dochází[260]. Vzhledem k těmto principům tak v jiném případě nebylo povoleno ani umístění kamery na oděvu zaměstnance, které by snímaly jeho činnost v desetisekundových intervalech[261].

7.1.2 Monitoring pohybu zaměstnanců

Využití kamerového systému připadá v úvahu zejména v provozovně zaměstnavatele a jejím nejbližším okolí. V souvislosti s nástupem ekonomické krize však přistoupili zaměstnavatelé k další možnosti kontroly zaměstnanců (zejména za účelem úspory nákladů), a to v podobě monitoringu pohybu služebních vozidel za využití systému GPS (Global Positioning Systém) či podobné služby. Ke sledování pohybu zaměstnanců může sloužit také lokace služebních telefonů právě prostřednictvím GPS, resp. obdobné služby, jež (zjednodušeně) umožňuje zaznamenávat pohyb zařízení, do něhož je vysílač signálu zabudován[262]. Protože i údaje o místě či místech, na nichž se subjekt údajů pohyboval, jsou osobními údaji ve smyslu Zákona[263], je na místě se jimi v souvislosti s ochranou osobních údajů zaměstnanců také zabývat.

Je jistě nezpochybnitelné, že zaměstnavatel má právo mít přehled o pohybu svých zaměstnanců během pracovní doby (často je tento systém využíván u obchodních zástupců, servisních techniků či profesionálních řidičů), neboť v podstatě nemá jinou možnost, jak kontrolovat výkon práce těch zaměstnanců, kteří se vzhledem k náplni svých pracovních úkolů obvykle nezdržují na jednom stálém pracovišti. Z tohoto důvodu je možné na GPS monitoring nahlížet jako na přiměřený způsob kontroly zaměstnanců vzhledem k absenci jiného, vůči soukromí

[259] Výroční zpráva ÚOOÚ za rok 2007, s. 29.
[260] Výroční zpráva ÚOOÚ za rok 2008, s. 59-60.
[261] Viz Výroční zpráva ÚOOÚ za rok 2010, s. 46.
[262] Pro zjednodušení bude v následující stati uvažována pouze geolokace pomocí GPS, neboť ostatní služby pracují na podobném principu.
[263] Srov. Stanovisko WP 185 ke geolokačním službám inteligentních mobilních zařízení, s. 7.

zaměstnanců méně invazivního nástroje. Zaměstnavatel sice může kupříkladu požadovat od zaměstnanců podrobné zprávy o náplni pracovní doby, nicméně vzhledem k obtížné zfalšovatelnosti dat získaných prostřednictvím GPS mají tyto údaje pro zaměstnavatele vysokou hodnotu, a také kromě dalšího i důkazní váhu, pokud by zaměstnavatel chtěl z výsledků jejich zpracování vyvodit pracovněprávní důsledky. Jako tomu však bylo v případě kamerových systémů, i u používání geolokačních služeb bude úkolem zaměstnavatele nastavit parametry monitoringu tak, aby splňovaly svůj účel a zároveň nezasahovaly do soukromí zaměstnanců více, než je nezbytně nutné. V úvahu tak namísto konstantního sledování může přicházet kupříkladu služba alarmu pro zaměstnavatele v případě, kdy sledovaný objekt překročí během pracovní doby hranice vymezeného území, nebo také tehdy, když se naopak subjekt delší dobu nepohybuje[264].

Účelem využití GPS monitoringu zaměstnanců bude nejčastěji úspora nákladů; obzvláště u používání motorových vozidel je jakékoliv využití tohoto pracovního prostředku k soukromým účelům vzhledem k cenám pohonných hmot i opotřebení vozidla pro zaměstnavatele značně citelné. Využití GPS proto zaměstnavateli umožňuje zjišťovat aktuální polohu vozidla, jakož i historii jeho pohybu; jedná se v podstatě o automatické vedení elektronické knihy jízd bez ingerence zaměstnance[265]. Dalším z účelů lokace zaměstnance může být však i jeho vlastní bezpečnost, a to například v případě terénních pracovníků pohybujících se v rizikových či odlehlých a těžko dostupných oblastech, jakož i prevence krádeží firemních vozidel či jiné trestné činnosti (při převozu peněz, osob atd.). Ve výše uvedených případech je dle mého názoru využívání tohoto způsobu kontroly zaměstnanců s ohledem na ustanovení § 316 odst. 2 zákoníku přípustné, a to i bez souhlasu zaměstnanců. Zaměstnanci, kteří k výkonu své práce využívají monitorované pracovní prostředky, však samozřejmě musí být o tomto

[264] Srov. Stanovisko WP 185 ke geolokačním službám inteligentních mobilních zařízení, s. 14.
[265] Monitorovací systém obvykle využívá přijímač signálu GPS, který určuje přesnou polohu v čase ve zvoleném intervalu a tyto informace ukládá do paměti. Následným přehráním do speciálního programu pak lze vytvořit podrobný itinerář jízd, včetně vyhodnocení spotřeby vozidla. Srov. Bartík, V., Janečková, E. *Ochrana osobních údajů v aplikační praxi.* 2. vyd. Praha: Linde, 2010, s. 153.

monitoringu řádně informováni a u zaměstnavatele musí být jasně stanovená pravidla pro zpracování takto získaných osobních údajů. Uplatní se rovněž i oznamovací povinnost dle ust. § 16 Zákona (oznamovací povinnosti však nebudou podléhat případy, kdy je GPS vysílač do služebních vozidel sice nainstalován, avšak aktivuje se pouze v případě odcizení vozidla či za obdobné situace). Na druhou stranu však není přípustné instalovat GPS lokátor do jakýchkoliv pracovních pomůcek, které to umožňují, byť třeba i se souhlasem zaměstnance. Jejich využití je odůvodněné výhradně v případech, kdy zaměstnavatel objektivně nemá trvale jinou možnost zaměstnance během jeho pracovní doby kontrolovat – absolutně proto není přípustné monitorovat pohyb zaměstnanců kdykoliv opustí své pracovní místo (např. z důvodu pracovní pochůzky) či dokonce pomocí GPS vysílače zjišťovat, zda se zaměstnanec zdržuje v místě svého bydliště v době nemoci či při práci z domova.

Problémy však i u odůvodněného monitoringu vzniknou v situaci, kdy je na základě dohody zaměstnanec oprávněn využívat služební vozidlo (resp. jiný pracovní prostředek sledovaný pomocí GPS) i k soukromým účelům. Některé systémy sice umožňují dočasnou deaktivaci GPS zařízení, jejich pořízení je však spojeno s vyššími náklady. Rovněž se může stát, že zaměstnavatel umožní používání vozidla k osobním potřebám až v době, kdy je již systém nainstalován. Záznam pohybu zaměstnance ve chvílích jeho privátního života je však zcela nepřípustný; zaměstnavatel by takto mohl získat značné množství v pracovněprávních vztazích zneužitelných údajů – například informace o návštěvách kostela, nemocnice a podobných zařízeních, jakož i délce (vzhledem k absenci pohybu vysílače) pobytu v nich[266]. V případě, že je GPS lokátor nainstalován nikoliv v automobilu, nýbrž v mobilním telefonu či laptopu zaměstnance, může být zásah do soukromí zaměstnance v případě sledování jeho pohybu ještě vyšší – obzvláště mobilní telefon nosí uživatelé většinu času ve své těsné blízkosti. Z tohoto důvodu by jakékoliv zařízení, které hodlá zaměstnavatel monitorovat a u něhož se dá předpokládat, že jej zaměstnanec bude využívat či mít

[266] Stanovisko WP 185 ke geolokačním službám inteligentních mobilních zařízení, s. 7.

při sobě i mimo svou pracovní dobu, mělo zaměstnanci umožňovat vypnutí této funkce po skončení pracovní doby.

I v případě údajů o pohybu zaměstnanců není zaměstnavatel oprávněn uchovávat tyto údaje déle, než je nezbytné pro splnění účelu jejich zpracování – tedy zejména ověření, že zaměstnanec využívá pracovní prostředky stanoveným způsobem a ve stanoveném rozsahu (nejčastěji zda používá služební vozidlo pouze k plnění pracovních úkolů). Ani v tomto případě není možné stanovit paušálně dobu, po jejímž uplynutí by zaměstnavatel byl povinen tato data smazat, neboť v závislosti na typu poskytované služby bude zaměstnavatel získávat shromážděné údaje v různě dlouhých období. Tato doba, po níž následuje vyhodnocení zjištěných údajů, by však neměla být nepřiměřena dlouhá; v úvahu bude zpravidla přicházet doba jednoho měsíce. Ihned poté, co jsou souhrnné údaje za dané období zaměstnavatelem ze systému získány a analyzovány (nejdéle však do několika málo pracovních dnů), by mělo následovat jejich nevratné smazání, ledaže by zjištěné výsledky měly zaměstnavateli posloužit jako důkazní prostředek k uplatnění svých oprávněných zájmů (např. vůči finančnímu úřadu či ve sporu se zaměstnancem).

7.1.3 Kontrola využívání elektronické pošty

Vedle monitoringu chování a pohybu zaměstnance přichází v úvahu kontrola výstupů, jež zaměstnanec na pracovišti odesílá a přijímá prostřednictvím elektronické pošty. Na prvním místě je třeba uvést, že elektronická pošta je považována za písemnost ve smyslu § 40 občanského zákoníku a jako taková podléhá listovnímu tajemství zaručenému již zmiňovaným článkem 13 Listiny základních práv a svobod[267], který zaručuje každému také kromě listovního tajemství i tajemství jiných písemností a záznamů uchovaných v soukromí, zasílaných poštou či jiným způsobem (tedy i elektronickou poštou), jakož i tajemství práv podávaných telefonem, telegrafem či podobným zařízením. Ani

[267] Bartík, V., Janečková, E. Ochrana soukromí na pracovišti – e-mailová pošta. *Práce a mzda.* 2009, č. 11, s. 28.

právo zaměstnavatele kontrolovat využití pracovní doby a jeho zájem na efektivní práci zaměstnanců tak neodůvodňují jakýkoliv zásah do tohoto ústavně zaručeného práva ze strany zaměstnavatele. Porušení tajemství dopravovaných zpráv dokonce může představovat skutkovou podstatu trestného činu podle ustanovení § 182 zákona č. 40/2009 Sb., trestního zákoníku[268].

Toto pojetí je rovněž v souladu se směrnicí č. 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, podle níž jsou veškeré informace uchovávané na koncovém zařízení uživatelů sítí elektronických komunikací součástí soukromí uživatelů vyžadujících stejnou úroveň ochrany jako kterékoliv další osobní údaje. Tato směrnice rovněž zdůrazňuje, že jakékoliv použití nástrojů umožňujících sledování aktivity uživatelů na síti může vážně narušit soukromí těchto uživatelů a mělo by tedy být povoleno pouze k oprávněným účelům s vědomím těchto uživatelů. Obecně by tedy monitoring činnosti zaměstnanců s využitím prostředků elektronické komunikace či internetu měl být stejně jako jakýkoliv jiný způsob sledování zaměstnanců využíván pouze v odůvodněných případech a o tomto sledování by měli být zaměstnanci vždy informováni. Jakékoliv systematické zpracování těchto údajů také podléhá Zákonu a nese s sebou kromě dalšího i oznamovací povinnost dle ustanovení § 16 Zákona.

S ohledem na výše uvedené proto zaměstnavatel nemá právo sledovat ani jinak zpracovávat obsah korespondence svých zaměstnanců, a to ani tehdy, pokud na pracovišti panuje přísný zákaz využívání počítačů a dalších elektronických zařízení k soukromým účelům a zábavě[269]. Mezi odbornou veřejností však panuje shoda, že zaměstnavatel může evidovat počet příchozích a odchozích e-mailů, a pokud pro to má oprávněný důvod (např. při vzniku podezření na zneužívání emailu, nedodržování pracovní doby atp.) i údaje o adresátech a odesílatelích[270]. O

[268] Dokument sub. pozn. č. 267, s. 29.
[269] Mališ, P. Ochrana osobních údajů na pracovišti a povinnosti zaměstnavatelů. *Personální a sociálně právní kartotéka.* 2009, č. 12, s. 5.
[270] Tamtéž, jakož i dokument sub. pozn. č. 265 nebo Stanovisko ÚOOÚ č. 2/2009 – Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště.

skutečnosti, že je příchozí a odchozí pošta monitorována, by ale zaměstnanci měli být informováni (např. individuálně v pracovní smlouvě či jejím dodatku nebo vnitřním předpisem, kde může zaměstnavatel také stanovit pravidla pro užívání e-mailových adres a přístupu na internet ze zaměstnavatelem poskytnutých IT zařízeních), a to hned při vzniku pracovněprávního vztahu[271], resp. před započetím monitorování, je-li na pracovišti zavedeno až v pozdější době.

Výjimečně se zaměstnavatel může seznámit i s *obsahem* pracovního e-mailu, a to tehdy, pokud nelze z objektivních důvodů zajistit, že se zaměstnanec se zprávou seznámí včas, aniž by zaměstnavateli hrozila újma z nezpracování takové zprávy[272]. O takové případy se bude jednat především v případě dlouhodobého onemocnění zaměstnance nebo tehdy, pokud by zaměstnanec ve výpovědní době bojkotoval své pracovní úkoly (zde by ovšem v závislosti na závažnosti „bojkotu" bylo na místě okamžité zrušení pracovního poměru s takovým zaměstnancem). Výše uvedená pravidla vycházejí z konstantního názoru Úřadu, nicméně se zde nabízí přirovnání s listovní obchodní korespondencí, kde již ustáleně platí: je-li dopis adresovaný společnosti a až na druhém místě je uvedeno jméno zaměstnance (zejména proto, aby se dokument dostal rychleji k odpovědné osobě v rámci společnosti), jedná se o obchodní korespondenci a zaměstnavatel je oprávněn takovou korespondenci otevřít a její obsah zpracovat (např. prostřednictvím recepce)[273]. Toto však pro e-mailovou poštu vzhledem k výše uvedenému neplatí, což dle mého názoru představuje značnou překážku při uplatňování práv zaměstnavatele. Nahlížení do e-mailové pošty zaměstnanců, doručené na jejich firemní e-mail, by mělo být přípustné i v dalších odůvodněných případech (např. podezření ohledně porušování obchodního tajemství), je-li o takovém oprávnění zaměstnavatele zaměstnanec informován, ve společnosti platí zákaz používání firemního mailu pro soukromé účely a z předmětu či oslovení adresáta konkrétního e-mailu nevyplývá, že by se mělo jednat o zprávu ryze soukromého charakteru;

[271] Dokument sub. pozn. č. 267, s. 30.
[272] Stanovisko ÚOOÚ č. 2/2009 – Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště.

etické by rovněž bylo zaměstnance na otevření zprávy upozornit a otevření e-mailu zaměstnavatelem zdůvodnit. Pokud by však z předmětu či jiných okolností bylo zřejmé, že se o soukromou zprávu jedná, je zaměstnavatel povinen od čtení zprávy dále upustit[274]. Jestliže by však zaměstnavatel takto narazil na větší počet soukromých zpráv, bylo by možné zaměstnance za takové jednání s přihlédnutím k dalším okolnostem postihnout[275].

Zcela se však ztotožňuji s názorem Úřadu v případě, který byl popsán ve Výroční zprávě Úřadu pro rok 2010[276] a který zcela jednoznačně označuje za nepřípustné, je-li e-mailová schránka zaměstnance aktivní i po skončení jeho pracovněprávního vztahu a příchozí zprávy jsou zaměstnavatelem otevírány (často bývají příchozí zprávy také přesměrovány do schránky jiného zaměstnance), a to obvykle bez vědomí dotyčného bývalého zaměstnance. V tomto případě není skutečně možné argumentovat ochranou oprávněných zájmů zaměstnavatele, neboť je nasnadě po odchodu bývalého zaměstnance tuto schránku zrušit s nastavením automatické odpovědi obsahující kontaktní údaje jiného zaměstnance. Lze však také připustit, aby bylo se zaměstnancem před skončením jeho pracovního poměru sjednáno, že veškerá příchozí pošta na jeho firemní mailovou adresu bude po skončení jeho působení u zaměstnavatele přesměrována do jiné firemní mailové schránky. Je potom v zájmu tohoto zaměstnance, aby veškerou svou případnou soukromou komunikaci, která přes tuto pracovní adresu probíhala, včas „odklonil" na svou adresu privátní. I v tomto případě však platí, že otevírání očividně soukromých zpráv zaměstnance (byť bývalého a přeposlaných do poštovní schránky jiného) je vyloučeno.

---

[273] Srov. dokument sub pozn. č. 217, jakož i rozhodnutí Českého telekomunikačního úřadu čj. 40106/05-608 ve znění pozdějších souvisejících rozhodnutí.
[274] Morávek, J. Kdy je možné evidovat přístup zaměstnance na internet a otevřít jeho e-mailovou poštu? *Právo pro podnikání a zaměstnání.* 2010, č. 3, s. 7.
[275] Bělina, M. a kol. *Zákoník práce. Komentář.* 2. vyd. Praha: C.H. Beck, 2010, s. 820.
[276] Viz Výroční zpráva ÚOOÚ za rok 2010, s. 27-28.

7.1.4 Sledování využívání internetu

Zaměstnavatel není oprávněn žádným způsobem sledovat, jaké webové stránky zaměstnanec navštěvuje, jestliže k tomu není dán (stejně jako u ostatních způsobů monitoringu zaměstnanců) zvláštní důvod spočívající v povaze jeho činnosti[277]. Zaměstnavatel však dle mého názoru může anonymně (tj. tak, že data jsou zpracovávána pouze souhrnně a jednotlivé výsledky není možné přiřadit ke konkrétnímu zaměstnanci) zaznamenávat přístupy na jednotlivé webové stránky a dobu strávenou jejich prohlížením, byť i k takovémuto „statistickému" sledování zaujímá Úřad zdrženlivý postoj[278]. O monitoringu využívání internetu by samozřejmě měli být zaměstnanci informováni, a to i s ohledem na zvýšení efektivity zákazu využívání internetu pro soukromé účely. Programy, které takové sledování umožňují, jsou stále populárnějším produktem na trhu softwaru, a pouze malé procento zaměstnavatelů pohyb zaměstnanců na internetu nikterak nekontroluje či vůbec neomezuje. Přiřazení získaných výsledků ke konkrétnímu zaměstnanci je přípustné upravit například v pracovním řádu pro případy, kdy přístup na „volnočasové" stránky překročí určité procento pracovní doby. V žádném případě však nelze připustit, aby zaměstnavatel využíval zařízení umožňující sledování dotyků na klávesnici. Toto již zcela jistě překračuje meze oprávněných zájmů zaměstnavatele a může představovat významné porušení práv zaměstnance a zásah do jeho soukromí (např. porušení listovního tajemství).

Oproti poměrně striktnímu přístupu Úřadu existuje již k této problematice také několik rozhodnutí soudů prvního i druhé stupně, které vyjádřily názor, že sledování pohybu zaměstnanců na internetu není při dodržení určitých podmínek v rozporu s právem na ochranu soukromí a že je zaměstnavatel při výrazných excesech oprávněn na základě údajů získaných s pomocí takového softwaru dovodit vůči zaměstnanci pracovněprávní důsledky (tj. zejména skončení pracovního poměru). Postoj soudů ke zneužívání internetu pro osobní účely

[277] Stanovisko ÚOOÚ č. 2/2009 – Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště.
[278] Stanovisko ÚOOÚ č. 2/2009 – Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště: část c) – Webové stránky.

naznačuje mimo jiné i rozhodnutí Okresního soudu v Jindřichově Hradci[279] z roku 2010, jenž označil za platné okamžité zrušení pracovního poměru se zaměstnancem, který během jednoho měsíce více než 65% pracovní doby strávil prohlížením webových stránek absolutně nesouvisejících s jeho pracovními úkoly, což zaměstnavatel zjistil na základě využití monitorovacího softwaru (údajně provozovaného dokonce bez vědomí zaměstnanců). Soud však průlomově toto sledování neshledal nezákonným, neboť program zaznamenával pouze navštěvované webové adresy; nesledoval však dotyky na klávesnici či obsahy e-mailové korespondence. Dne 22.2.2011 bylo toto rozhodnutí potvrzeno Krajským soudem v Českých Budějovicích (sp.zn. 19 Co 260/2011), který rovněž sledování navštívených webových stránek nepovažoval za zásah do osobnostních práv zaměstnance, a to ačkoliv o něm nebyli zaměstnanci informováni. Dle údajů z veřejné přístupného informačního systému[280] bylo proti tomuto rozhodnutí podáno dovolání k Nejvyššímu soudu[281] a bude velice zajímavé sledovat, jaký verdikt v této záležitosti zazní a jak bude rozhodnutí odůvodněno.

S internetovým surfováním v pracovní době souvisí také rozhodnutí Nejvyššího soudu sp.zn. 21 Cdo 1839/2008 ze dne 5.5.2009. V tomto svém rozsudku Nejvyšší soud potvrdil rozhodnutí nižších soudů, které shledaly porušení pracovní kázně zvlášť hrubým způsobem (slovy současného ZP „porušení povinnosti vyplývající z právních předpisů vztahujících se k vykonávané práci zvlášť hrubým způsobem“) v tom, že zaměstnanec ve funkci ředitele pobočky bankovního ústavu opakovaně po dobu sedmi měsíců prohlížel webové stránky, jejichž obsah nesouvisel s pracovními povinnostmi, a navíc několikrát neoprávněně nahlížel na účty klientů. Z odůvodnění rozsudku však vyplývá, že za hlavní prohřešek soud považoval nahlížení na bankovní účty a s tím v důsledku spojené narušení nezbytné důvěry, kterou ve vedoucího zaměstnance

[279] Viz např. http://m.ihned.cz/c4-10132710-49532750-700000_hndetail-kontrola-zamestnancu-versus-soukromi-bod-pro-firmy.
[280] http://infosoud.justice.cz
[281] Řízení bylo zahájeno dne 18.5.2011 a je vedeno pod sp.zn. 21 Cdo 1771/2011.

zaměstnavatel měl, nicméně ani prohlížení stránek nesouvisejících s pracovní náplní soud v tomto případě rozhodně nepovažoval za irelevantní.

Nejlevnějším a právně nejjistějším způsobem, jak zabránit zneužívání internetu pro soukromé účely zaměstnanců a také tím, jenž by měl být primárně upřednostňován[282], tak prozatím i nadále zůstává neposkytnutí přístupu k internetu těm zaměstnancům, kteří jej pro své pracovní úkoly nepotřebují, resp. zablokování těch webových stránek a domén, které s pracovními úkoly nesouvisejí. Zaměstnavatelé by si však měli být také vědomi skutečnosti, že není možné a ani efektivní naprosto celou pracovní dobu strávit plněním pracovních úkolů a že malé odreagování zaměstnanců, jestliže k němu nedochází na úkor pracovních výsledků, jejich pracovní efektivitu nikterak neohrozí, naopak ji často i zvýší.

7.1.5 Monitoring telefonátů

Pro kontroly telefonátů platí obdobné zásady jako v případě e-mailové pošty; i telefonickým odposlechem nejen soukromých, ale i obchodních hovorů totiž může dojít k narušení soukromí odposlouchávaných osob[283]. Zaměstnavatel tak není zejména oprávněn bez vědomí a souhlasu zaměstnance odposlouchávat a nahrávat obsah jeho telefonických rozhovorů. K odposlouchávání či dokonce nahrávání telefonních hovorů by mělo docházet zásadně se souhlasem zaměstnance, a to pouze ve výjimečných a řádně odůvodněných případech (např. tehdy, uzavírá-li zaměstnanec po telefonu smlouvy s klienty a pro případné spory o jejich obsahu je nezbytné, aby byl hovor zaznamenán). Pokud jde o výpisy telefonních čísel, na která zaměstnanec volá, případně, z nichž hovory přijímá, jejich monitorování je ze strany zaměstnavatele v zásadě přípustné, neboť mu umožňuje dohled nad nakládáním s pracovními prostředky, které byly zaměstnanci svěřeny (pevná linka, SIM karta), a také do určité míry umožňuje sledování využití

[282] Dokument sub. pozn. č. 274.
[283] Srov. např. Rozsudek Evropského soudu pro lidská práva ve věci Huvig proti Francii ze dne 24.4.1990 nebo rozsudek téhož soudu ve věci Halford proti Spojenému království ze dne 25.6.1997.

pracovní doby zaměstnancem[284]. I v takovém případě by však měl být zaměstnanec o tomto monitorování informován a vnitřním předpisem či podobným způsobem by měla být jasně stanovená pravidla pro (ne-)využívání služebních telefonů k soukromým účelům. Nedodržování těchto pravidel pak může být ze strany zaměstnavatele vyhodnoceno jako porušení povinností vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci (tzv. pracovní kázeň) a odpovídajícím způsobem sankcionováno[285].

7.1.6 Biometrická identifikace zaměstnanců

Biometrické údaje jsou informace, které získáme měřením či snímáním určitých charakteristických prvků či projevů lidského těla. Mezi nejpoužívanější biometrické údaje tak patří například výška, váha, barva vlasů či očí; biometrickým údajem je však také styl písma či vada řeči. Některé z biometrických údajů však samy o sobě umožňují přímou identifikaci nebo autentizaci subjektů, neboť jsou pro každou bytost jedinečné; tyto údaje jsou pak údaji citlivými, neboť na základě znalosti tohoto jediného konkrétního údaje je možné jednak dotyčnou osobu takřka nezaměnitelně identifikovat a jednak o ní v případě některých biometrických údajů získat značné množství dalších informací. Typickými biometrickými údaji používanými k identifikaci bývají otisky prstů či dlaní, struktura sítnice, rohovky či hlasu. Kriminalistické metody pak využívají i celou řadu dalších charakteristických prvků člověka, jako jsou např. způsob chůze, geometrie obličeje a další.

Na rozdíl od jiných způsobů monitorování zaměstnanců na pracovišti není dosud biometrická identifikace zaměstnanců mezi zaměstnavateli příliš využívána. Důvodem je zejména vysoká finanční náročnost technologií, jež biometrickou identifikaci umožňují; dá se však očekávat jejich rozšíření, a to zejména tehdy, bude-li pořizovací cena srovnatelná s výhodami, které zaměstnavateli biometrická identifikace přinese, obdobně jako tomu bylo v případě kamerových systémů.

[284] Bartík, V., Janečková, E. *Ochrana osobních údajů v aplikační praxi.* 2. vyd. Praha: Linde, 2010, s. 151.

V současnosti je použití biometrické identifikace upraveno pro speciální případy pouze vyhláškou č. 144/1997 Sb., o fyzické ochraně jaderných materiálů a jaderných zařizování, která stanoví biometrickou identifikaci osoby jako podmínku vstupu do střeženého prostoru s jadernými reaktory (např. geometrií ruky či otiskem prstů). Databáze vstupů je dostupná jeden měsíc, poté se blokuje a po uplynutí jednoho roku je zlikvidována. Obdobně si lze význam biometrické identifikace představit také u zaměstnanců majících přístup k utajovaným informacím[286], nejspíše však nikoliv plošně u všech či velké většiny zaměstnanců, a to s ohledem na princip proporcionality, který platí při jakémkoliv sledování zaměstnance (výše zmiňovaný § 316 odst. 2 ZP). Tento přístup potvrzuje také Úřad, když ve své Výroční zprávě za rok 2007 odmítl použití biometrické identifikace na místě běžné evidence (např. docházky) na pracovišti, neboť by rozsah zpracování údajů byl vzhledem k účelu nepřiměřený[287]. Úřad rovněž upozornil, že pro účely autentizace osob není rozhodně nutné uchovávat tyto citlivé údaje v centrální databázi a doporučuje jejich decentralizované archivování[288]. Používání biometrických systémů, které neuchovávají stopy v paměti terminálu přístupového zařízení a ani je neukládají do centrální databáze, podporuje také Pracovní skupina 29[289].

I přes svou stále poměrně značnou finanční náročnost jsou však biometrické údaje v současnosti stále šířeji využívány jako tzv. identifikátory, a to vzhledem k jejich schopnosti jednoznačné identifikace jedince a neměnnosti v čase jako identifikátory velice spolehlivé – čipovou kartu zaměstnance může použít k přístupu na pracoviště nebo i do zabezpečené IT-centrály někdo jiný, heslem může disponovat i jiná osoba než vlastník, otisk prstu či hlasovou stopu však ničím jiným nahradit nelze. Jak však varuje Pracovní skupina 29 a na lokální úrovni i

[285] Tamtéž.
[286] Stanovisko ÚOOÚ č. 3/2009 – Biometrická identifikace nebo autentizace zaměstnanců.
[287] Výroční zpráva ÚOOÚ za rok 2007, s. 42.
[288] Stanovisko ÚOOÚ č. 3/2009 – Biometrická identifikace nebo autentizace zaměstnanců.
[289] Pracovní dokument WP 80 o biometrii, s. 4.

Úřad, s plošným rozšiřováním systémů identifikace[290] na základě biometrických údajů i v běžných situacích[291] hrozí, že si společnost přestane uvědomovat velké riziko zneužití těchto údajů a jejich poskytování třetím osobám přestane považovat za vysoce senzitivní[292]. I proto by se biometrika založená na zpracování citlivých údajů v centrální databázi měla využívat pouze ve výjimečných a odůvodněných případech[293]. Zaměstnavatelé také nesmí zapomínat, že trvalé ukládání biometrických údajů je možné jako jakékoliv jiné zpracování citlivých údajů pouze za podmínek stanovených v § 9 Zákona, tj. nejčastěji s výslovným souhlasem subjektu údajů. Pouze tehdy, dochází-li k biometrické identifikaci osoby povinně na základě zákona, uplatní se výjimka podle § 9 písm. d) Zákona[294].

Ne vždy se však v případě využívání biometrické identifikace musí jednat o zpracování citlivých údajů. Pro předcházení možnostem zneužití těchto citlivých údajů se totiž správcům, kteří k jejich využití přistupují, vysoce doporučuje provést pouhý otisk biometrického údaje např. za pomoci hash funkce. V takovém případě je zjednodušeně řečeno biometrický znak ihned po jeho sejmutí/zjištění převeden do jedinečného číselného kódu, z něhož není možné zpětně daný biometrický údaj reprodukovat, a samotný biometrický znak je ihned zlikvidován. Při všech dalších identifikačních procesech se tak vždy daný biometrický znak identifikované osoby, aniž by někde byl zaznamenáván, převede do číselného kódu a při identifikaci tak dochází ke srovnání těchto dvou kódů a nikoliv k porovnání samotného biometrického znaku s jeho záznamem[295]. V takovém případě se proto nebude jednat o zpracování citlivých údajů; jelikož je však daný číselný kód přiřaditelný ke konkrétní osobě, je potřeba s ním nakládat jako s ostatními osobními údaji[296]. Pokud navíc takové zpracování osobních údajů bude sloužit

[290] Zatímco v případě procesu identifikace dochází k přesnému určení dané osoby (tj. výběru z neurčitého množství dat uložených v systému), výsledkem procesu autentizace je ověření, že daná osoba je osobou, za níž se vydává (dochází tedy pouze k porovnání údaje uloženého v systému s biometrickým údajem dotyčné osoby).
[291] Např. při vstupu do veřejných budov.
[292] Pracovní dokument WP 80 o biometrii, s. 2.
[293] Dokument sub. pozn. č. 286.
[294] Srov. tamtéž.
[295] Pracovní dokument WP 80 o biometrii, s. 10.
[296] Srov. dokument sub. pozn. č. 286.

k plnění práv a povinností vyplývajících z pracovněprávních vztahů (např. při zpracování evidence pracovní doby), nebude ani nutné takové zpracování osobních údajů oznamovat Úřadu, neboť je na danou situaci možné aplikovat výjimku podle ustanovení § 18 odst. 1 písm. b) Zákona[297].

7.2 Předávání osobních údajů zaměstnanců do zahraničí

Další otázky, kterými jsou v současnosti zaměstnavatelé nuceni se zabývat, vyvstávají v souvislosti s jejich potřebou předávání osobních údajů zaměstnanců do zahraničí. Důvody zaměstnavatelů k předávání osobních údajů do zaměstnanců mohou být v podstatě dvojí[298]: jednak tehdy, jsou-li data předávána do zahraničí za účelem zpracování (tj. zaměstnavatel jako správce uzavře smlouvu o zpracování se zahraničním zpracovatelem) a jednak tehdy, děje-li se tak pro potřeby zahraničního subjektu (typicky mateřská společnost), a to zejména za účelem provádění centralizovaných analýz, na jejichž základě bude mateřská společnost schopna stanovit správnou strategii řízení celého koncernu a efektivní rozmístění pracovních sil v rámci jednotlivých společností. Zaměstnavatelé – správci údajů si však musí být vědomi toho, že i předání osobních údajů zaměstnanců dalšímu subjektu je dalším způsobem jejich zpracování, a proto k němu musí dát zaměstnanci souhlas, neboť se pravděpodobně neuplatní žádná zákonná výjimka ve smyslu § 5 odst. 2 Zákona. Stejně tak předávání podléhá i oznamovací povinnosti vůči Úřadu podle § 16 Zákona.

Pojmem předání lze přitom rozumět jakýkoliv akt, prostřednictvím něhož jsou osobní údaje fyzicky předány (včetně elektronického předání) zahraničnímu subjektu pro další zpracování. V dnešní době samozřejmě valná většina předání osobních údajů probíhá elektronickou cestou; o předání tedy nepůjde v tom případě, budou-li údaje druhé osobě pouze *zpřístupněny*, samotný přenos dat však

[297] Viz také dokument sub. pozn. č. 286.
[298] Srov. Bartík, V., Janečková, E. *Ochrana osobních údajů v aplikační praxi.* 2. vyd. Praha: Linde, 2010, s. 173.

bude vyloučen[299] (typicky tzv. virtuální data roomy neumožňující stahování ani kopírování údajů v nich obsažených). V takovém případě hovoříme o zpřístupnění údajů, nicméně i to lze provádět pouze se souhlasem subjektu údajů nebo na základě zákonného oprávnění. O předání údajů do zahraničí se nebude jednat ani v případě, kdy jsou data uložena na serveru nacházejícím se ve třetím státě, k nimž však nemá nikdo z této třetí země přístup. Půjde například o situaci, kdy se server bude nacházet v centrále mateřské společnosti, nicméně uložené osobní údaje budou přístupné pouze pověřeným pracovníkům české dceřiné společnosti[300].

Předání osobních údajů do jiných států Zákon upravuje v ustanovení § 27, z něhož vyplývá, že osobní údaje lze předávat do zahraničí v zásadě pouze s povolením ÚOOÚ, což však neplatí ve třech případech. První případ se opírá o ustanovení § 27 odst. 1, podle něhož je možné předávat osobní údaje do ostatních členských států Evropské unie bez omezení. Toto ustanovení transponuje čl. 1 odst. 2 Směrnice, který stanoví, že členské státy nemohou omezit ani zakázat volný pohyb osobních údajů mezi členskými státy[301]. Z tohoto důvodu je nutné výraz „členské státy", jakož i „třetí země" vykládat v souladu se Směrnicí, jež je závazná nejen pro členské státy Evropské unie, ale i zbylé členské země Evropského hospodářského prostoru[302]. Jelikož přijetí a provedení Směrnice garantuje adekvátní úroveň ochrany, jsou všechny země tvořící Evropský hospodářský prostor[303] považovány za „bezpečné", a osobní údaje mezi nimi mohou být předávány bez jakýchkoliv dalších omezení[304].

---

[299] Srov. Kučerová, A. Nonnemann, F. *Ochrana osobních údajů v otázkách a odpovědích.* 1. vyd. Praha: BOVA POLYGON, 2010, s. 76.; Morávek, J. *Ochrana osobních údajů v pracovněprávní agendě.* 1. vyd. Praha: BMSS Start, 2010, s. 71.

[300] Matoušová, M. a kol. *Ochrana osobních údajů v otázkách a odpovědích.* 1. vyd. Praha: ASPI Publishing, 2004, s. 65.

[301] Bartík, V., Janečková, E. *Zákon o ochraně osobních údajů s komentářem.* 1. vyd. Olomouc: ANAG, 2010, s. 196.

[302] Srov. Dohoda o Evropském hospodářském prostoru ze dne 2.5.1992 a rozhodnutí Smíšeného výboru EHP č. 83/1999 ze dne 25. června 1999, kterým se mění protokol 37 a příloha XI Dohody o EHP.

[303] Tj. členské státy EU spolu s Islandem, Lichtenštejnskem a Norskem.

[304] Srov. Morávek, J. BCR (Binding Corporate Rules). *Právo pro podnikání a zaměstnání.* 2009, č. 9, s. 8.

Dalším případem, kdy není nutné žádat Úřad o povolení (byť se nejedná o předání v rámci EU), je podle druhého odstavce § 27 předávání osobních údajů do třetích zemí, pokud zákaz omezování volného pohybu osobních údajů vyplývá z mezinárodní smlouvy, k jejíž ratifikaci dal Parlament souhlas, a kterou je Česká republika vázána. Zde se zejména jedná o státy, které ratifikovaly Úmluvu č. 108 a jejich právní řády by tedy měly garantovat minimální ochranu osobní údajů dle mezinárodních standardů (v rámci Evropské unie jsou minimální požadavky stanoveny Směrnicí)[305].

Posledním případem nevyžadujícím povolení Úřadu je předávání osobních údajů do třetích zemí určených na základě rozhodnutí orgánu Evropské unie, jímž je Komise. Rozhodnutí Komise, která se týkají například Švýcarska, Argentiny či Izraele, prakticky znamenají, že při předávání osobních údajů do těchto zemí není zapotřebí žádat Úřad o povolení, neboť legislativní ochranu osobních údajů v dané zemi označila Komise ve svém rozhodnutí jako odpovídající[306]. Další rozhodnutí Komise se týkají USA[307] a Kanady[308] a jsou do jisté míry specifická, neboť v případech předávání osobních údajů do těchto států je nejprve nutné zkoumat, zda se jedná o případ pokrytý příslušným rozhodnutím[309]. Posledním „balíčkem" rozhodnutí v této kategorii jsou rozhodnutí Komise týkající se standardních smluvních doložek – rovněž při použití jednoho typu standardních smluvních doložek není zapotřebí žádat povolení Úřadu k předání údajů do třetích zemí (k tomu více viz. subkapitola 7.2.2).

Jestliže však daný případ předání nespadá ani pod jeden ze tří výše uvedených případů, může být předání uskutečněno pouze na základě povolení Úřadu tehdy, prokáže-li správce splnění některé z podmínek uvedených v § 27

[305] Dokument sub. pozn. č. 301, s. 197.
[306] Srov. www.uoou.cz / Předávání osobních údajů do zahraničí / Přehled případů předávání osobních údajů do zahraničí, u nichž není nutno žádat Úřad o povolení.
[307] Rozhodnutí Komise ze dne 26.7.2000 o odpovídající ochraně poskytované podle zásad „bezpečného přístavu" a s tím souvisejících „často kladených otázek" vydaných Ministerstvem obchodu USA
[308] Rozhodnutí Komise ze dne 20.12.2001 podle Směrnice o odpovídající ochraně osobních údajů, kterou poskytuje kanadský zákon o ochraně osobních informací a elektronických dokumentech
[309] Srov. dokument sub. pozn. č. 301, s. 197.

odst. 3 Zákona[310]; splnění podmínky přitom musí být prokazatelně doloženo[311]. Výčet důvodů (podmínek) pro předání osobních údajů je prakticky shodný s okruhem důvodů pro zpracování osobních údajů v případech, kdy povinnost jejich zpracování neukládá správci právní předpis. Osobní údaje tak mohou být předávány do jiných zemí, na které se neuplatní žádná z výše uvedených výjimek, jedině

- se souhlasem nebo na základě pokynu subjektu údajů, nebo
- pokud jsou v třetí zemi, kde mají být údaje zpracovány, vytvořeny dostatečné zvláštní záruky ochrany osobních údajů (např. použití smluvní doložky, avšak nikoliv v podobě tzv. standardní smluvní doložky na základě rozhodnutí Komise, nebo systém tzv. vnitropodnikových závazných pravidel), nebo
- pokud jsou předávané osobní údaje součástí veřejně přístupných datových souborů, a to na základě zvláštního zákona, nebo
- pokud je předání nutné pro uplatnění důležitého veřejného zájmu vyplývajícího ze zvláštního zákona nebo mezinárodní smlouvy / nezbytné pro plnění smlouvy uzavřené v zájmu subjektu údajů / nezbytné pro ochranu práv nebo životně důležitých zájmů subjektu údajů (zejména pro záchranu života nebo poskytnutí zdravotní péče)[312].

O povolení je správce povinen požádat Úřad ještě před započetím předávání údajů (§ 27 odst. 4). Na základě žádosti správce pak zahájí Úřad správní řízení podle zákona č. 500/2004 Sb., správní řád, jehož výsledkem je rozhodnutí o (ne)povolení předání osobních údajů v konkrétním případě. O žádosti musí Úřad dle správního řádu[313] rozhodnout ve lhůtě 30 dnů, ve složitějších případech pak 60 dnů. Povolení je obvykle vydáváno na dobu určitou (nejčastěji 2 až 3 roky). Při

[310] A zároveň nestanoví-li zvláštní zákon jinak; takovým zákonem je např. zákon č. 273/2008 Sb., o Policii České republiky (§ 80 odst. 9) nebo zákon č. 359/1999 Sb., o sociálně-právní ochraně dětí (§ 35 odst. 3).
[311] Srov. dokument sub. pozn. č. 301, s. 197.
[312] Tento výčet je pouze zjednodušeným a zkráceným přepisem ustanovení § 27 odst. 3 Zákona.
[313] § 71 odst. 3 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů

posuzování žádosti přezkoumává Úřad zejména zákonnost a účelnost předávání údajů a jejich rozsah, neboť poměrně často dochází v rámci skupiny propojených osob (koncerny) k předávání osobních údajů v nadbytečném rozsahu a mateřské společnosti navíc vyžadují, aby jim údaje byly předávány v neanonymizované podobě[314]. Neuvědomují si však, že subjekty údajů (tj. zaměstnanci dceřiné či sesterské společnosti sídlící v České republice) nejsou vůči mateřské společnosti v žádném pracovněprávním ani podobném vztahu, a jejich osobní údaje by tak měly být předávány de facto cizí osobě. Podle názoru Úřadu tak zahraničním mateřským společnostem mohou být předkládány ekonomické souhrny obsahující anonymizované údaje zaměstnanců a v případech smluvně garantované spolupráce může koncernová společnost obdržet i údaje o konkrétních pracovnících. Správcům žádajícím o povolení ve smyslu § 27 odst. 4 Zákona Úřad doporučuje, aby přihlédli zejména k tomu, že

1. problematika předávání osobních údajů do zahraničí je limitována nejen podmínkami stanovenými v Zákoně, nýbrž musí být také v souladu s právním řádem České republiky, a to včetně předpisů Evropské unie;

2. účel a případné meze nakládání s údaji zaměstnanců jsou stanoveny také zákoníkem práce a dalšími právními předpisy (např. pro účely vedení personální a mzdové agendy);

3. chce-li společnost vyhodnocovat osobní údaje pro účely racionalizace práce a efektivity činnosti v rámci celého koncernu, je povinna osobní údaje anonymizovat, neboť účelem jejich zpracování je analýza vedoucí ke zlepšení hospodářských výsledků zaměstnavatele, resp. celého koncernu. Pokud by společnost zpracovávala neanonymizovaná data za účelem uspokojení svých ekonomických potřeb, byl by překročen rámec stanovený právními předpisy, neboť by způsob zpracování nebyl přiměřený účelu, jehož

[314] Viz www.uoou.cz / Předávání osobních údajů do zahraničí / K problémům z praxe.

má být zpracováním dosaženo. Tento rozpor s právními předpisy přitom nemůže zhojit ani souhlas zaměstnance[315].

Při předávání osobních údajů v rámci (nejen) koncernových společností může docházet také ke komplikacím při určení příslušného dozorového úřadu či vymezení vzájemného vztahu mezi předávajícími osobami. Obvykle se jedná o situaci české dceřiné společnosti a zahraniční matky (pro zjednodušení předpokládejme, že se její sídlo nachází v rámci EU). Často bývají osobní údaje zaměstnanců zpracovávány právě centrálně u zahraniční matky a společnosti mívají problém určit, která společnost má za povinnost podat oznámení vůči dozorujícímu Úřadu. Právě v takovém případě bude záležet na vymezení vzájemného postavení obou společností[316] – nositelem oznamovací povinnosti je totiž zásadně správce. Dle konstantního výkladu Úřadu je jedinou výjimkou z tohoto pravidla situace, kdy osobní údaje zpracovává tuzemský subjekt jako zpracovatel pro zahraničního správce a přitom za zpracování dat na území České republiky je odpovědný pouze zpracovatel, správce do něj v podstatě nijak nezasahuje. V tomto případě bude pro dohled nad daným způsobem zpracování příslušný český Úřad a nositelem oznamovací povinnosti bude český zpracovatel[317].

V případě vztahu správce – zpracovatel jsou společnosti navíc povinny uzavřít smlouvy o zpracování podle § 6 Zákona. V rámci koncernu však může být samozřejmě i dceřiná společnost v postavení správce, resp. obě společnosti mohou být správci současně. Posouzení bude záviset na charakteru jejich vzájemného vztahu a na vymezení jednotlivých úkolů, resp. kdo tyto úkoly a rozsah zpracování bude z pozice správce určovat. Každý článek celé soustavy však musí zaručit dostatečná opatření při zabezpečení ochrany zpracovávaných údajů.

[315] Tamtéž.
[316] Srov. Stanovisko ÚOOÚ č. 2/2010 – Předání osobních údajů do jiných států.
[317] Srov. dokument sub. pozn. č. 300, s. 63.

7.2.1 Safe Harbor

Protože Spojené státy americké nedisponují žádnou všeobecně platnou legislativou, jež by zajišťovala ochranu osobních údajů v privátním sektoru[318] (je zde tradičně dáván prostor pro samoregulaci této problematiky), a nemá tak ani zřízen žádný dozorový orgán v této oblasti, byl faktickou smlouvou mezi Spojenými státy americkými a Evropskou komisí založen institut Safe Harbor neboli „bezpečný přístav", a to v podobě Rozhodnutí Komise ze dne 26.07.2000, které stanoví, že společnosti zahrnuté do seznamu Safe Harbor jsou svými systémy ochrany osobních údajů (v podobě přijatých technických a administrativních opatření) konformní se Směrnicí[319].

Americké společnosti spadající do kompetence Federální obchodní komise (Federal Trade Commission - FTC) nebo Ministerstvu dopravy (Department of Transportation)[320] se mohou dobrovolně přihlásit k dodržování zásad Safe Harbor podáním žádosti k Ministerstvu obchodu USA (U. S. Department of Commerce) o zařazení do seznamu, na základě níž jsou poté zařazeny do on-line přístupného a pravidelně aktualizovaného seznamu[321]. Účast v seznamu musí společnosti každoročně potvrzovat prohlášením vůči ministerstvu o tom, že splňují stanovené požadavky, které představují určitý komplex technických a administrativních opatření (*self-regulatory privacy programme / policy*).

K provádění těchto požadavků vydalo americké Ministerstvo pokyny v podobě přehledu otázek a odpovědí (FAQ), které podrobněji rozvádí sedm základních principů Safe Harbor. Těmi jsou zjednodušeně řečeno informační povinnost (*notice*), dobrovolnost (*choice*), splnění podmínek i na straně příjemce údajů (*onward transfer*), právo na přístup k údajům (*access*), zabezpečení údajů

[318] Kučerová, A. Nonnemann, F. *Ochrana osobních údajů v otázkách a odpovědích.* 1. vyd. Praha: BOVA POLYGON, 2010, s. 74.
[319] Srov. Stanovisko ÚOOÚ č. 2/2010 – Předání osobních údajů do jiných států.
[320] Program Safe Harbor není přístupný většině finančních institucí, telekomunikačních společností, neziskovým organizacím či zemědělským sdružením.
[321] Viz https://safeharbor.export.gov/list.aspx.

(*security*), aktuálnost a přesnost údajů (*data integrity*) a vymahatelnost principů (*enforcement*)[322].

Kontrolu nad dodržováním těchto principů provádí zejména Federální obchodní komise; v prosinci roku 2008 však byla konzultantskou společností Galaxia provedena studie funkčnosti systému Safe Harbor[323], v níž bylo konstatováno, že myšlenka Safe Harbor je prozatím spíše přáním, jak by spolupráce mezi USA a členskými státy EU v oblasti předávání osobních údajů měla fungovat, než skutečně funkčním systémem. Za nejzásadnější nedostatek bylo označeno neplnění základních zásad ze strany participujících společností a nedostatečný výkon dozoru. Na základě této zprávy a dalších jednání mezi zástupci Evropské komise a amerických institucí byly prosazeny určité kroky směřující ke zlepšení celého systému a v roce 2009 došlo ze strany FTC k postihu šesti společností, které se klamavě označovaly za účastníky programu Safe Harbor[324]. I nadále je však nedodržování zásad účastnickými společnostmi velkým problémem celého systému[325].

Zaměstnavatelům, kteří hodlají předávat osobní údaje zaměstnanců do Spojených států amerických a ověří, že se osoba, jíž mají být údaje předány, nachází na seznamu „Safe Harbor“, se proto doporučuje další prověření – například zda je certifikace dané osoby stále platná, zda jsou „privacy policy“ této společnosti veřejně přístupné (nejčastěji prostřednictvím webu) a zda společnost dodržuje principy Safe Harbor[326]. V případě pochybností je na místě konzultace s Úřadem, zda skutečně k předání není zapotřebí jeho povolení.

[322] Srov. např. http://export.gov/safeharbor/eu/eg_main_018476.asp.
[323] The US Safe Harbor – Fact or Fiction, dostupné z http://www.galexia.com/public/research/articles/research_articles-pa08.html.
[324] Viz např. http://www.ftc.gov/opa/hsr-safeharbor.shtom.
[325] Srov. Výroční zpráva ÚOOÚ za rok 2008, s. 80.
[326] Stanovisko ÚOOÚ č. 2/2010 – Předání osobních údajů do jiných států.

7.2.2 Standardní smluvní doložky

Dalším ze způsobů, jak se tuzemští správci osobních údajů mohou zbavit povinnosti žádat Úřad o povolení k uskutečnění předání osobních údajů do třetích zemí, je začlenění standardní smluvní doložky podle některého z vícera rozhodnutí Evropské komise do smluvního podkladu mezi nimi a osobou, které jsou údaje předávány. V praxi tak předávající strana (označovaná jako vývozce) uzavře s přijímající stranou (dovozcem) nacházejícím se ve třetí zemi smlouvu o předání osobních údajů, jejíž nedílnou součástí je i standardní smluvní doložka[327]. Výběr doložky přitom záleží na rozhodnutí stran a charakteru jejich vzájemného vztahu (správce – správce[328] / správce – zpracovatel); doložky však nesmí být nijak změněny ani kombinovány mezi sebou. Smlouva o předání osobních údajů však může obsahovat i další doložky, které ale se standardními smluvními doložkami nesmí být v rozporu[329]. Vzhledem k tomu, že při použití doložek strany nemají povinnost žádat o povolení Úřadu k předání, se může ovšem stát, že se Úřad o jednotlivých předáních vůbec nedozví a případné porušení co do použití doložek nezjistí.

Původní Rozhodnutí Komise o standardních smluvních doložkách pro předávání zpracovatelům[330] bylo v roce 2010 nahrazeno novým, aktuálnějším rozhodnutím[331], které rozvinulo problematiku tzv. řetězení zpracovatelů. V souladu s tímto rozhodnutím tak může zpracovatel údajů ve třetí zemi, jemuž byly údaje předány (tj. dovozce údajů), pověřit částí zpracování další subjekt mimo EU, který se tak dostane do pozice dílčího zpracovatele. Podmínkou pro tento postup je

[327] Standardní smluvní doložky jsou přílohou jednotlivých rozhodnutí Komise.
[328] Rozhodnutí Komise ze dne 15.6.2001 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle směrnice 95/45/ES (2001/497/ES). Na základě použití této doložky jsou oba správci solidárně odpovědni vůči subjektu údajů za jakékoliv případné porušení smlouvy (viz doložka 6).
[329] Stanovisko ÚOOÚ č. 2/2010 – Předání osobních údajů do jiných států.
[330] Rozhodnutí Komise ze dne 27.12.2001 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice 95/46/ES (2002/16/ES).
[331] Rozhodnutí Komise ze dne 5.2.2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES (2010/87/EU).

předchozí písemný souhlas správce údajů, který údaje předává (tj. vývozce), a existence písemné smlouvy mezi zpracovatelem a dílčím zpracovatelem, v níž jsou dílčímu zpracovateli uloženy stejné povinnosti ohledně ochrany osobních údajů, jakými je vázán sám zpracovatel. Plnou odpovědnost vůči správci údajů však má vždy prvotní zpracovatel, který tak odpovídá i za porušení zásad zpracování na straně dílčího zpracovatele[332]. Správce sám je pak odpovědný vůči subjektu údajů jak za jednání prvotního, tak dílčí, resp. jakéhokoliv dalšího zpracovatele. Pouze v případě, kdy by nebylo možné uplatnit odpovědnost vůči správci (např. z důvodu zániku bez právního nástupce či platební neschopnosti), přechází odpovědnost vůči subjektu postupně na prvotního a poté případně i dílčího zpracovatele.

Ani po vydání Rozhodnutí Komise z roku 2010 však zatím není řešena situace, kdy budou data předána zpracovatelem z členského státu EU dílčímu zpracovateli z třetí země. V takovém případě tedy musí správce údajů uzavřít standardní smluvní doložku přímo s dílčím zpracovatelem z třetí země, k níž přistoupí i EU-zpracovatel.

7.2.3 Binding Corporate Rules

Závazná podniková pravidla, obecně označovaná anglickým výrazem Binding Corporate Rules („BCR“), představují jeden z možných prostředků zvláštní záruky ve smyslu § 27 odst. 3 písm. b) Zákona při předávání osobních údajů v případě, že jsou tyto údaje předávány v rámci jednoho a téhož nadnárodního podnikatelského uskupení (koncernu) do třetích zemí, které nezajišťují odpovídající úroveň ochrany osobních údajů. Jako jednu z možností zajištění adekvátní úrovně ochrany předvídá vytvoření Binding Corporate Rules i čl. 26 odst. 2 Směrnice[333]. Na rozdíl od použití standardních smluvních doložek či využití institutu Safe Harbor však přijetí BCR nezbavuje správce

[332] ÚOOÚ k problémům z praxe č. 2/2010 – Dílčí zpracovatel osobních údajů dle rozhodnutí Komise 2010/87/EU ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES.

[333] Viz www.uoou.cz / Předávání osobních údajů do zahraničí / K problémům z praxe / Závazná podniková pravidla (Binding Corporate Rules) jako nástroj bezpečného předávání osobních údajů do třetích zemí.

povinnosti opatřit si před uskutečněním předání povolení Úřadu. Obzvláště pro velké nadnárodní společnosti se sesterskými či dceřinými společnostmi po celém světě však BCR představují praktický (byť zpočátku administrativně náročnější) způsob, jak zajistit možnost předávání osobních údajů mezi jednotlivými společnostmi, a to i do zemí mimo EU[334]. Problematice BCR je také věnovaná značná pozornost Pracovní skupiny 29.

Závazná podniková pravidla jsou ve své podstatě jakousi smlouvou mezi podnikatelským uskupením a příslušným národním úřadem o tom, že ze strany uskupení budou dodržovány deklarované principy nakládání s osobními údaji včetně jejich předávání do třetích zemí a že bude zajištěna adekvátní ochrana těchto údajů[335]. Většinou jsou tvořena základním dokumentem, který obsahuje všechny principy ochrany osobních údajů tak, jak vyplývají ze Směrnice, jakož i další standardy, které jsou vzorově uvedeny v řadě pracovních dokumentů Pracovní skupiny 29[336]. Mateřská společnost, která hodlá závazná podniková pravidla přijmout, se musí zavázat, že budou pravidla přijata v celém koncernu a že bude zajištěno jejich dodržování prostřednictvím zavedených dozorových mechanismů. Jak však uvádí Úřad ve své Výroční zprávě za rok 2010, tato pravidla bývají často pouze deklarovaná, přičemž následná kontrola jejich dodržování ze strany odpovědného subjektu by prokázala značné mezery. Problémem však bývá, že při případné kontrole ze strany Úřadu by musela být navázána spolupráce s dalším úřadem, který je garantem pro naplnění obecně platných povinností na území třetího státu[337].

Postup při vytváření BCR je následující[338]: mateřská společnost si nejprve musí zvolit (a také tuto volbu odůvodnit) vedoucí dozorový úřad (anglicky *Data Protection Autority* - DPA), přičemž jako kritérium slouží především sídlo centrály celé skupiny; pomocná kritéria pak představuje místo, odkud bude nejčastěji o zpracování

[334] Srov. dokument sub. pozn. č. 298, s. 177.
[335] Morávek, J. BCR (Binding Corporate Rules). *Právo pro podnikání a zaměstnání*. 2009, č. 9, s. 9.
[336] Dokument sub. pozn. č. 335, s. 8.
[337] Srov. Výroční zpráva ÚOOÚ pro rok 2010, s. 11.
[338] Viz Pracovní dokument WP 107 o spolupráci při vydávání společných stanovisek k přiměřeným zárukám vyplývajícím ze závazných podnikových pravidel, s. 2.

rozhodováno, nebo místo, odkud bude předávání údajů do dalších zemí nejčastěji uskutečňováno. Společnost následně vyplní formulář podle Pracovního dokumentu WP 133 a podá jej u zvoleného dozorového úřadu; ten posoudí, zda má právě on být skutečně vedoucím dozorovým úřadem[339] (*Lead Authority*). Společnost musí také vedoucímu dozorovému úřadu poskytnout jakékoliv další dokumenty, z nichž vyplývá její závazek k dodržování BCR[340]. Na rozdíl od samotných BCR však v žádosti o schválení[341] musí být také uvedeno a doloženo vysvětlení, jak bude dosaženo závaznosti pravidel pro jednotlivé členy skupiny i jejich zaměstnance, a doklad, že společnost, která převezme odpovědnost i za členy skupiny se sídlem mimo EU, disponuje dostatečným majetkem, který by ji případně umožnil nahradit škody vzniklé z porušení BCR[342]. Společnost totiž musí v závazných podnikových pravidlech také určit odpovědnou osobu v rámci celé skupiny se sídlem v EU, která převezme odpovědnost za případná porušení člena skupiny se sídlem mimo EU[343]. Pokud to není objektivně možné, připouští WP 29 i zavedení jiného odpovědnostního mechanismu v rámci skupiny, který bude lépe vyhovovat struktuře a konkrétním podmínkám koncernu (např. solidární odpovědnost, zajištění odpovědnosti prostřednictvím standardních smluvních doložek)[344]; zároveň však zdůrazňuje použití této výjimky pouze ad hoc a v případech, kde žadatel poskytne dostatečné záruky ochrany zájmů subjektu údajů[345].

Pokud vedoucí úřad shledá svou příslušnost, rozešle vyplněný formulář ostatním dotčeným dozorovým orgánům. Pokud tyto orgány nebudou mít k úmyslu vytvoření BCR žádné námitky, započne vedoucí úřad spolupráci se společností na vypracování návrhu BCR. Hotový návrh se posléze zašle všem dotčeným úřadům k připomínkám,

[339] Srov. dokument sub. pozn. č. 335, s. 9.
[340] Demonstrativní výčet dokumentů k předložení DPA je obsažen například v Pracovním dokumentu WP 154 o společném rámci pro strukturu závazných podnikových pravidel, s. 10.
[341] Rozdíly mezi obsahem žádosti a samotnými pravidly jsou přehledně znázorněny v Pracovním dokumentu WP 153 s tabulkou prvků a zásad závazných podnikových pravidel.
[342] Pracovní dokument WP 108 stanovící modelový seznam pro žádost o souhlas s vydáním závazných podnikových pravidel, s. 4 a 6.
[343] Odpovědným členem skupiny by měla být mateřská společnost. Jestliže se však její sídlo nenachází v členském státě EU, je za skupinu zvolena jiná společnost v rámci EU, která tuto odpovědnost převezme (srov. WP 154, s. 9, jakož i Pracovní dokument WP 74, s. 18).
[344] Pracovní dokument WP 154, s. 9, pozn. č. 7.
[345] Pracovní dokument WP 155 o často kladených otázkách (FAQs) týkajících se závazných podnikových pravidel (BCR), s. 3.

které mohou vyjádřit do 30 dnů od doručení návrhu BCR[346]. Vzhledem k dvojímu obracení se na všechny dotčené dozorové orgány je celý výše uvedený postup časově značně náročný; v praxi se proto často postupuje proto bez předchozí konzultace dotčených orgánů k úmyslu vytvoření BCR, neboť v této fázi obvykle žádné připomínky nejsou. Návrh BCR se poté dotčeným orgánům zasílá společně i s určením vedoucího dozorového orgánu[347]. I tak bývá schvalovací procedura spíše delší, neboť vzhledem k menším zkušenostem některých národních úřadů se vedoucí úřad setkává s řadou připomínek, a to někdy i dokonce protichůdných (neboť se národní úřady snaží o upřednostňování vlastní národní úpravy[348]), což schvalovací proces značně prodlužuje.

Při vypracovávání BCR může společnost postupovat dle rámcové struktury publikované skupinou WP 29[349]; jak sama Pracovní skupina 29 ale upozorňuje, její Pracovní dokument WP 154 nepředstavuje vzorové BCR. BCR by tak zejména měla obsahovat cíle a rozsah zpracovávaných údajů, základní definice (odpovídající terminologii Směrnice), závazek zpracovávat údaje pouze v nezbytném rozsahu a přiměřenými způsoby, právní rámec pro samotné zpracování, a to jak osobních, tak citlivých údajů, právo subjektů na informace o zpracování, na přístup ke zpracovávaným údajům, právo požadovat jejich výmaz či blokování, a také zabezpečení a důvěrnost osobních údajů. BCR by rovněž měla obsahovat úpravu vztahů správce se zpracovateli, jež jsou součástí celé skupiny, jakož i pravidla pro předání osobních údajů externím zpracovatelům. Pravidla by měla také stanovit postup dohledu nad svým dodržováním, sankční mechanismus a vnitřní systém podávání stížností a oznamování podezření na porušení pravidel[350].

Ne vždy však mohou společnosti začít se zpracováváním a zejména předáváním osobních údajů ihned po schválení Binding Corporate Rules. Tato možnost totiž závisí na tom, zda v sobě mají jednotlivé národní právní řády zakotvenou pojistku obdobnou

[346] Pracovní dokument WP 107, s. 3.
[347] Srov. dokument sub. pozn. č. 335, s. 9.
[348] Výroční zpráva ÚOOÚ za rok 2008, s. 81.
[349] Pracovní dokument WP 154.
[350] Srov. dokument sub. pozn. č. 335, s. 9.

ustanovení § 27 odst. 4 Zákona, tj. podmínku žádat národní dozorový úřad před započetím předávání o povolení k předání. Přestože na první pohled taková podmínka působí jako obstrukce celého procesu, ve skutečnosti může schvalovací proceduru dokonce urychlit – státy, které mohou využít této poslední pojistky, často necítí potřebu rozsáhlého připomínkování návrhu BCR, neboť si jsou vědomi své možnosti uplatnění BCR v případě potřeby na území „svého" státu zabránit[351]. I český ÚOOÚ opakovaně upozorňuje, že „schválení BCR nevylučuje povinnost poboček společností usazených v ČR požádat Úřad o povolení předávání osobních údajů do třetích zemí ve smyslu § 27 Zákona, kdy bude opětovně (a tentokrát nikoli jen v obecné rovině) zkoumáno, zda BCR v modifikaci pro Českou republiku splňují podmínky uložené § 27 odst. 3 písm. b) Zákona pro bezpečné předávání osobních údajů do třetích zemí". Úřad rovněž zdůrazňuje, že posouzení BCR v případě, kdy je Úřad pouze jedním z dotčených úřadů, je pouze předběžné, a že v případě zájmu o předávání osobních údajů na základě těchto BCR z České republiky do třetích zemí bude třeba Úřad požádat o povolení na základě § 27 odst. 4 Zákona[352].

7.3 Whistleblowing

Posledním problémem, kterým bych se zde chtěla zabývat, je doposud nepříliš diskutovaná otázka tzv. whistleblowingu[353]. Potřeba otevřít tuto problematiku se v evropských zemích objevila v návaznosti na zákon přijatý Kongresem USA v roce 2002 pod názvem Sarbanes-Oxley Act („SOX"), jehož vydání bylo podníceno řadou finančních podvodů[354] uvnitř amerických společností[355]. Termínem whistleblowing tak byl zprvu označován interní systém

[351] Srov. dokument sub. pozn. č. 335, s. 10.
[352] Výroční zpráva ÚOOÚ za rok 2008, s. 81.
[353] Jedním z prvních pojednání v české literatuře k tomuto tématu byl soubor tří článku J. Pichrta a J. Morávka v periodiku *Právo pro podnikání a zaměstnání* v průběhu roku 2009. Na stránkách mezinárodních advokátních kanceláří se však v poslední době objevuje nemálo newsletterů zabývajících se touto problematikou (viz např. www.whitecase.com/hrhottopic_1107/ nebo www.schonherr.eu/news-publications/publications/checkliste-whistleblowing).
[354] Symbolem whistleblowingu se na počátku tohoto tisíciletí stal Harry Markopolos (často označován jako „Madoff Whistleblower"), který se mnoho let marně snažil upozorňovat úřady na zřejmé finanční podvody probíhající ve společnosti Bernard L. Madoff Investment Securities a z toho plynoucí ohrožení vkladů investorů.
[355] Srov. Stanovisko WP 117, s. 5.

kontroly zavedený společnostmi, které buď přímo pocházejí, nebo jsou podílově vlastněny a ovládány společnostmi se sídlem ve Spojených státech amerických[356] – právě takovým společnostem bylo zavedení oznamovacího systému uloženo zákonem SOX – nicméně v současnosti dochází k zavádění interních oznamovacích kanálů[357] i v evropských společnostech, které zákonu SOX nepodléhají, což ovšem souvisí s rozšířením tohoto mechanismu v důsledku přijetí SOX.

Nejvíce problematickou oblastí se v souvislosti se zaváděním systému whistleblowingu ve společnostech působících v EU ukázala být otázka ochrany osobních údajů pramenící z odlišných pojetí této problematiky v Evropě a USA[358] – evropské společnosti, které chtěly dostát svým povinnostem, jež jim ukládá SOX, se ocitly v jakési schizofrenní situaci: svým jednáním se totiž mohly zároveň dopustit porušení předpisů na ochranu osobních údajů platných v zemích EU; v opačném případě jim zase hrozila sankce z titulu nedodržení amerického zákona SOX[359]. K prvním střetu rozdílných přístupů k ochraně osobních údajů v EU a USA došlo v květnu 2005, kdy francouzský dozorový úřad rozhodl, že hotlinka zřízená pro účely whistleblowingu ve společnosti McDonald's Inc. porušuje francouzské předpisy na ochranu osobních údajů. Francouzský úřad přitom argumentoval zejména nerespektováním práv zaměstnanců společnosti, kteří by se stali předmětem oznámení, jakož i rizikem velkého počtu falešných oznámení s cílem poškození pověsti ostatních zaměstnanců; úřad nicméně zároveň naznačil, za jakých podmínek je připraven zavedení tohoto systému akceptovat[360].

[356] Stanovisko WP 117 tímto pojmem označuje vnitřní postupy oznamování podezření z protiprávního jednání", a to zejména v oblasti účetnictví, auditu, boje proti úplatkářství a trestné činnosti v bankovním a finančním sektoru.
[357] V anglicky psané literatuře se pro tyto kanály vžilo označení „hotlines".
[358] V této souvislosti bývá nejčastěji uváděn zvýšený důraz na ochranu soukromí v Evropě v důsledku negativních zkušeností učiněných během druhé světové války či komunistických režimů v jednotlivých zemích.
[359] Srov. Stanovisko WP 117, s. 5.
[360] Viz rozhodnutí CNIL (Commission Nationale de l´Informatique et des Libertés) č. 110-2005 ze dne 26.05.2005. Přestože od té doby došlo k několika registracím systému whistleblowingu u francouzského dozorového úřadu (ten mezitím vydal vlastní směrnici ve vztahu ke whistleblowingu), v prosinci 2009 rozhodl francouzský kasační soud (Cour de cassation) o protiprávnosti systému ve společnosti Dassault Systèmes z důvodu jeho neomezeného rozsahu

V Německu zase shledal soud[361] protiprávní zavedení hotlinky ve společnosti Wal-Mart, neboť k němu došlo bez předchozí konzultace se zástupci zaměstnanců, přestože celý systém klade na zaměstnance další nároky[362]. Zejména francouzská rozhodnutí, jakož i skutečnost, že ze samotného principu fungování tohoto systému bylo možné předpokládat, že bude docházet ke zpracování a převádění osobních údajů ze států EU do USA, podnítila Pracovní skupinu WP 29, složenou z vedoucích kontrolních úřadů jednotlivých členských států, k vydání stanoviska k problematice whistleblowingu a pokynům k jeho zavádění ve společnostech se sídlem v EU při současném dodržování předpisů na ochranu osobních údajů[363]. Stanovisko Pracovní skupiny 29 zdůraznilo, že přestože může existovat oprávněný zájem zaměstnavatele na zavedení celého systému, je třeba mít při jeho realizaci na paměti princip proporcionality, neboť při něm zpravidla bude docházet k omezení práva určitých osob na soukromí, jakož i ochranu svých osobních údajů.

Výše zmíněný zákon SOX totiž požaduje, aby veřejné společnosti s americkou účastí a jejich pobočky (resp. organizační složky) nacházející se v členských státech EU, jakož i společnosti ze všech třetích zemí, jejichž akcie se obchodují na americké burze cenných papírů[364], vytvořily vnitřní systém umožňující příjem stížností a podnětů stávajících i bývalých zaměstnanců těchto společností, jejichž prostřednictvím má být upozorňováno na podezřelá (zejména

---

(rozhodnutí č. 2524 ze dne 08.12.2009). Více také příspěvek Eriky Collins ze společnosti Paul, Hastings, Janofsky & Walker LLP „Sarbanes-Oaxley: Whistle Blowing Provisions and Extra-Territorial Application z konference EELA (European Employment Lawyers Association) konané v Amsterdamu v květnu 2009, dostupný z www.eela.org/perl/fsystem.pl.

[361] ArbG Wuppertal, 15.06.2005, Az: 5 BV 20/05. Toto rozhodnutí bylo později potvrzeno odvolacím soudem, z něhož pochází i následující perlička: zákaz vztahů na pracovišti mezi nadřízenými a podřízenými zakotvený ve vnitřním předpisu společnosti byl soudem druhého stupně shledán v rozporu s německou ústavou (viz LAG Düsseldorf, 14.11.2005, Az: 10 TaBV 46/05).

[362] V této souvislosti se nabízí otázka nutnosti projednání s odborovou organizací či radou zaměstnanců zavedení systému whistleblowingu v české společnosti. Jelikož by k jeho zavedení došlo nejspíše vnitřním předpisem, jenž je zaměstnavatel oprávněn jednostranně vydat, i pokud u něj působí odborová organizace (viz § 305 odst. 1 ZP), není zřejmě projednání zavedení tohoto systému nutné.

[363] Srov. příspěvek Gerlinde Wisskirchen „Whistleblowing and Privacy Protection in Europe“ z konference Americké advokátní komory ve Philadelphii v listopadu 2007, dostupný z apps.americanbar.org/labor/annualcoonference/2007/materials/data/papers/v2/065.pdf.

[364] Srov. Stanovisko WP 117, s. 5.

protiprávní, avšak také nemorální či neetická) jednání v souvislosti s finančními toky ve společnosti, jichž se dopustili jejich spolupracovníci, nadřízení nebo obchodní partneři. Základní princip whistleblowingu spočívá tedy v tom, že osoba, která se při své běžné činnosti ve společnosti setká se škodlivým jednáním, oznámí tuto skutečnost prostřednictvím k tomu určeného zvláštního kanálu, který doplňuje obvyklé informační kanály uvnitř společnosti (zejména komunikace s vedoucími zaměstnanci či zástupců zaměstnanců)[365]. Informace, která je předmětem oznámení, se tak dostane buď příslušnému specializovanému oddělení zřízenému v rámci společnosti, nebo k externímu partnerovi, kterého společnost k prošetření whistleblowingu využívá. Charakteristickým znakem celého oznamovacího systému je tedy zjevně skutečnost, že během něj dochází ke zpracování osobních údajů[366] (tj. jejich shromažďování, uchovávání, předávání a další), a jako takový proto musí splňovat zákonem stanovené požadavky na jakékoliv zpracování osobních údajů (zákonnost zpracování – zde nejčastěji na základě zvláštního zákona nebo v případě jeho absence k ochraně oprávněného zájmu správce údajů, dále jeho proporcionalita a kvalita zpracovávaných údajů, soulad se stanoveným účelem, adekvátní míra zabezpečení apod.[367]).

K uskutečnění oznámení jsou zaměstnancům zpravidla k dispozici speciálně zřízené telefonní linky či webové aplikace; v některých společnostech jsou však omezeny skupiny osob, které mohou jednání oznámit, stejně tak jako osob, na které může být oznámení podáno[368]. Pro zpracování podaných oznámení a následného vyšetřování může společnost zřídit oddělenou jednotku uvnitř své interní struktury (toto oddělení by mělo obsahovat omezený počet speciálně vyškolených zaměstnanců tak, aby skutečně nebyly údaje zpřístupněny žádné neoprávněné osobě) nebo může jeho provozem pověřit externí subjekt, s nímž společnost uzavře smlouvu o poskytování této služby, jejíž součástí budou i

[365] Tamtéž.
[366] O osobní údaje by se nejednalo pouze tehdy, bylo-li by oznámení učiněno anonymně a současně by na jeho základě nebylo možné identifikovat konkrétní osobu. Je představitelné, že i na takovém oznámení by společnost mohla mít zájem, nicméně se nedá předpokládat, že by k takovým typům oznámení docházelo v praxi často.
[367] Srov. Stanovisko WP 117, s. 7.

všechny náležitosti běžné smlouvy o zpracování – tj. zejména povinnosti ve vztahu k ochraně a zabezpečení zpracovávaných osobních údajů, neboť i při pověření třetího subjektu nese společnost odpovědnost za to, jak je s údaji získanými v rámci systému nakládáno[369].

Velice důležitou součástí tohoto oznamovacího systému musí být i opatření poskytující ochranu oznamovateli před jakýmikoliv případnými postihy v souvislosti s podaným oznámením (v opačném případě by motivace k využití systému byla velice nízká), spočívající především v zachování důvěrnosti podaného oznámení včetně identity oznamovatele, neboť až na výjimečné případy nebývá dovoleno podávání anonymní oznámení a za případná úmyslně falešná oznámení bývají stanoveny sankce[370]. Na to, že anonymnost oznámení nemusí být vhodným řešením, upozorňuje i WP 29, a to mimo jiné také z toho důvodu, že vyšetřování celé záležitosti je z důvodu anonymity oznamovatele ztížené, neboť mu není možné klást doplňující otázky, a navíc ani anonymita mnohdy nezabrání tomu, že bude oznamovatelova identita zjištěna. Podle WP 29 není navíc anonymita oznámení v souladu s požadavkem nestranného shromažďování údajů, a proto zastává Pracovní skupina názor, že by prostřednictvím whistleblowingu mělo být připuštěno podávání výhradně neanonymních oznámení, resp. aby jejich podání bylo umožněno výhradně ve výjimečně odůvodněných případech a se zvláštní obezřetností příjemce[371].

Pracovní skupina 29 však také upozorňuje na stigmatizaci osob označených za škůdce bez ohledu na princip presumpce neviny, a s tím potenciálně spojené nedbalé či dokonce protiprávní nakládání s osobními údaji těchto osob. I přes případné obvinění z protiprávního jednání má každá osoba právo na ochranu a bezpečnost svých osobních údajů a ochranu soukromí a je velice důležité, aby mezi právy obou dotčených stran byla nastolena rovnováha[372]. Omezení základních

---

[368] Srov. Informační bulletin ÚOOÚ č. 4/2009, s. 6.
[369] Pichrt, J., Morávek, J. Whistleblowing. *Právo pro podnikání a zaměstnání*. 2009, č. 7-8, s. 22.
[370] Srov. Informační bulletin ÚOOÚ č. 4/2009, s. 4.
[371] Srov. Stanovisko WP 117, s. 11.
[372] Srov. Stanovisko WP 117, s. 13.

zásad ochrany osobních údajů je nutné aplikovat ve zcela výjimečných případech, je-li to nezbytně nutné k dosažení daného účelu (tj. řádnému prošetření oznámené události). Ochrana údajů osoby, která je předmětem oznámení, si zasluhuje o to větší pozornost vzhledem ke skutečnosti, že údaje této osoby nejsou na rozdíl od údajů oznamovatele zpracovávány na základě jejího souhlasu[373].

Osoba, vůči níž bylo podáno oznámení, má zejména právo na informace o zpracování svých osobních údajů. Odpovědná osoba v rámci systému by podezřelého měla co nejdříve informovat o tom, že proti němu bylo podáno oznámení, a poskytnout mu informace zejména o subjektu, který celý systém whistleblowingu řídí, o tom, z čeho je podezírán a jak může uplatnit své právo na přístup ke zpracovávaným údajům. Toto informační sdělení a poučení je možné odložit pouze v případě, kdy by tím bylo objektivně ohroženo vyšetřování a hrozilo by znehodnocení důkazů. Pokud se týká práva na podezřelé osoby na přístup ke svým údajům, jejich opravu a výmaz, nevztahuje se toto právo na poskytnutí totožnosti oznamovatele. Tu je možné odhalit pouze v případě, je-li zjištěno úmyslné podání nepravdivého oznámení[374]. Informace a osobní údaje získaná v souvislosti s podaným oznámením a jeho následným vyšetřováním by měla společnost dle názoru WP 29 zlikvidovat nejpozději do dvou měsíců od ukončení vyšetřování oznámeného skutku; to se však netýká těch případů, kdy bylo na základě zjištěných skutečností zahájeno soudní nebo jiné řízení (ať už s podezřelou osobou či s oznamovatelem, např. z důvodu podání nepravdivého oznámení)[375].

V souvislosti se zaváděním mechanismu whistleblowingu ve společnostech působících na území České republiky vyvstává také otázka, zda taková společnost jako správce osobních údajů podléhá oznamovací povinnosti ve smyslu § 16 Zákona. Přestože ustanovení § 18 odst. 1 písm. b) Zákona stanoví, že oznamovací povinnost se nevztahuje na zpracování osobních údajů, které správci ukládá

[373] Morávek, J. Whistleblowing – praktické otázky. *Právo pro podnikání a zaměstnání*. 2009, č. 11, s. 13.
[374] Srov. Stanovisko WP 117, s. 13.

zvláštní zákon (kterým by mohl být americký SOX), nelze dovodit, že by v tomto případě český zákonodárce odkazoval i na cizí právní předpisy a tím umožnil jejich působnost i na území České republiky. Z tohoto důvodu se tak na výše uvedené správce oznamovací povinnost vůči českému ÚOOÚ bude vztahovat, stejně jako by se vztahovala na jakoukoliv další společnost, jež by uvnitř své struktury systém whistleblowingu zavedla, aniž by sama podléhala působnosti zákona SOX[376].

Jelikož jsem si vědoma skutečnosti, že problematika whistleblowingu je v praxi velice komplikovaná, uvádím na závěr přehled základních bodů, jež by společnosti uvažující o zavedení „hotlinky" pro whistleblowing měly mít na zřeteli[377]:

- neumožnění nebo alespoň výrazné omezení možnosti anonymních oznámení;
- omezení předmětu oznámení pouze na nejzávažnější jednání, která mohou poškodit společnost jako celek;
- zajištění bezpečnosti údajů, jakož i ochrany identity oznamovatele a až do prošetření záležitosti také podezřelého;
- informování osoby, která je předmětem oznámení, jakož i dání prostoru k vyjádření druhé strany;
- omezená doba uchovávání shromážděných osobních údajů;
- dodržování všech dalších povinností správce osobních údajů, a to včetně oznamovací povinnosti vůči Úřadu.

Ve vnitřním předpise[378] upravujícím systém whistleblowingu by proto měly být dostatečně vysvětleny důvody, proč a za jakým účelem je systém ve společnosti zaváděn a nejlépe uvedeny příklady typů oznámení, k nimž je systém určen (například případy úplatkářství, objevení zásadních nesrovnalostí v účetnictví, podezření na trestnou činnost). V předpise by rovněž mělo být

[375] Srov. Stanovisko WP 117, s. 12.
[376] Srov. Morávek, J. Whistleblowing - zákonná opora. *Právo pro podnikání a zaměstnání*. 2009, č. 12, s. 17, jakož i Stanovisko WP 117, s. 17.
[377] Viz také www.natlawreview.com/article/employer-s-guide-to-implementing-eu-compliant-whistleblowing-hotlines.

uvedeno, že systém představuje pouze doplňkový informační kanál vedle již zavedených informačních mechanismů ve společnosti a pro „běžná“ oznámení týkající se například pracovního poměru konkrétního zaměstnance by měly být přednostně použity právě tyto tradiční cesty. Dále je zapotřebí popsat jednotlivé kroky celé procedury oznámení včetně těch zajišťujících utajení identity zaměstnavatele a zároveň zdůraznit, že falešná oznámení budou přísně sankcionována[379]. Zaměstnanci by také měli být informováni, komu budou údaje přijaté hotlinkou předávány, přičemž tyto osoby by měly být ke zpracování oznámení speciálně vyškoleny.

[378] Srov. pozn. č. 362.
[379] Viz také www.hrlaw.co.uk/site/toptips/leaks_in_the_pipeline.html.

Závěr

Přestože jsem se v předchozích kapitolách snažila zdůraznit aktuálnost a význam celé právní oblasti ochrany osobních údajů a byť se tímto tématem zabývá nemálo autorů, jsem zde bohužel nucena konstatovat, že v praxi bývá tato oblast stále vnímána jako okrajová problematika či nadstandard, který si mohou „dovolit" řešit pouze velké nadnárodní společnosti s týmem právníků v pozadí. K tomu přispívá i poměrně specifická terminologie a vágnost právní úpravy zejména ve vztahu ke zpracování osobních údajů moderními technologiemi, jíž vyplňují v podstatě jen stanoviska odborných orgánů. Zejména menší správci si proto často ani nejsou vědomi všech povinností, které jim právní úprava v souvislosti se zpracováním osobních údajů ukládá. Nejsou nicméně ojedinělé ani případy správců, kteří, byť jsou s danou právní úpravou seznámeni, své povinnosti spojené se zpracováním osobních údajů zcela opomíjí a riziko sankce ze strany kontrolních orgánů nepovažují za reálnou hrozbu. Tomuto bohužel napomáhá i současný stav, kdy veřejnost do jisté míry rezignovala na ochranu vlastních osobních údajů a své osobní údaje poskytuje komukoliv bez dalšího na vyžádání; někdy bývají dokonce udiveni, pokud od nich podnikatelský subjekt při své činnosti osobní údaje nevyžaduje či se jejich požadování snaží odůvodnit.

Je zřejmé, že nalezení rovnováhy mezi potřebou a zájmem zaměstnavatele zpracovávat osobní údaje svých zaměstnanců či uchazečů o zaměstnání a současně právem těchto osob na ochranu svých osobních údajů není jednoduché. Oproti jiným správcům ukládá zaměstnavatelům povinnost zpracovávat některé osobní údaje zákon, a proto se každý zaměstnavatel s plněním svých zákonných povinností automaticky ocitá v pozici správce osobních údajů se všemi důsledky s tím spojenými.

Zorientovat se v povinnostech, které právní předpisy se zpracováním osobních údajů spojují, není vždy snadné; to platí zejména tehdy, rozhodne-li se zaměstnavatel zpracovávat osobní údaje zaměstnanců nad rámec, který mu právní předpisy ukládají. Vzhledem k odlišnostem v povaze podnikatelských aktivit

různých zaměstnavatelů není samozřejmě dobře možné vytvořit jednoznačný manuál v oblasti nakládání s osobními údaji v pracovněprávních vztazích. Určité vodítko pro zaměstnavatele však může představovat kritérium proporcionality – je zpracování tohoto druhu osobních údajů zaměstnanců skutečně nutné? Musím tento údaj zpracovávat u všech zaměstnanců, resp. u všech ve stejném rozsahu a stejným způsobem? Nemohu dosáhnout stejného cíle i jinými prostředky?

Vždy je třeba také vycházet z premisy, že právo na soukromí a ochranu osobnosti je s každým jednotlivcem neoddělitelně spojeno. Je proto nutné odmítnout představu, že vstupem na své pracoviště zaměstnanec tato práva ztrácí a teprve po skončení pracovní doby jich nabývá zpět. I při výkonu zaměstnání má každý člověk právo na určitou míru soukromí, která musí být v každém případě ze strany zaměstnavatele respektována. S ohledem na oprávněné zájmy zaměstnavatele pak lze toto právo sice částečně omezit, vždy ale pouze v rozsahu, který je pro dosažení daného účelu nezbytně nutný.

Právě s použitím principu proporcionality, který respektuje jak ústavně zaručené právo jedince na osobní život a soukromí, tak i taktéž ústavně zaručené právo zaměstnavatele vlastnit majetek a zajišťovat jeho ochranu, jakož i právo na svobodné podnikání, jsem se v této práci pokusila o vyřešení některých sporných otázek v oblasti ochrany osobních údajů v pracovněprávních vztazích. Překotný společenský a technický vývoj nutí odvětví ochrany osobních údajů stejně jako další právní odvětví pružně reagovat na nově vznikající, právními předpisy nepředvídané situace. Je docela dobře možné, že témata, která v době vzniku této práce nebyla v popředí zájmu zaměstnavatelů (například zpracování biometrických dat zaměstnanců), budou za krátký čas nejpalčivější. Zcela jistě se objeví také otázky naprosto nové, na které bude teprve třeba hledat odpověď. Pokud však zaměstnavatel bude brát v úvahu princip přiměřenosti, jakož i další základní principy ochrany osobních údajů, kterými se tato práce zabývala, měl by s určitou minimální znalostí právní problematiky v dané situaci dospět k vhodnému, vyváženému a především zákonnému řešení.

Úkolem moci zákonodárné by pak za přispění odborné veřejnosti včetně Úřadu na ochranu osobních údajů mělo být dosažení stavu, kdy požadavky právní úpravy kladené na jednotlivé správce osobních údajů budou srozumitelné bez aplikačních nejasností a jejich dodržování nebude představovat neúměrně vysokou administrativní zátěž. Důležitým faktorem je rovněž nárůst povědomí o významu celé oblasti ochrany osobních údajů mezi veřejností. Ze všech důvodů, uvedených v této práci, bychom proto neměli připustit, aby se ochrana osobních údajů stala výsadou právní teorie, jíž se zabývají pouze státní orgány a mezinárodní instituce, ani aby se na právní úpravu této oblasti pohlíželo jen na jakousi deklaraci, jako se tomu v minulosti stalo kupříkladu u systému Safe Harbour, kdy se při pozdějších kontrolách jasně ukázalo, že praxe je zcela odlišná od principů deklarovaných v jednotlivých dokumentech.

Použitá literatura

Monografie

- D´AMBROSOVÁ, H. *Ochrana osobních údajů při vedení personálních agend.* 1. vyd. Praha: Pragoeduca, 2002.
- D´AMBROSOVÁ, H. *Ochrana osobních údajů v personalistice od roku 2005.* 1. vyd. Praha: Pragoeduca, 2005.
- BARTÍK, V., JANEČKOVÁ, E. *Zákon o ochraně osobních údajů s komentářem.* 1. vyd. Olomouc: ANAG, 2010.
- BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi.* 2. vyd. Praha: Linde, 2010.
- BĚLINA, M. a kol. *Zákoník práce. Komentář.* 2. vyd. Praha: C.H. Beck, 2010.
- HŮRKA, P. a kol. *Pracovní právo v bodech s příklady.* 2. vyd. Praha: Wolters Kluwer, 2010.
- KUČEROVÁ, A. BARTÍK, V. PECA, J. NEUWIRT, K., NEJEDLÝ, J. *Zákon o ochraně osobních údajů. Komentář.* 1. vyd. Praha: C. H. Beck, 2003.
- KUČEROVÁ, A. NONNEMANN, F. *Ochrana osobních údajů v otázkách a odpovědích.* 1. vyd. Praha: BOVA POLYGON, 2010.
- MAŠTALKA, J. *Osobní údaje, právo a my.* 1. vyd. Praha: C.H. Beck, 2008.
- MATES, P. *Ochrana osobních údajů.* 1. vyd. Praha: Karolinum, 2002.
- MATES, P. NEUWIRT, K. *Právní úprava ochrany osobních údajů v ČR.* 2. vyd. Praha: IFEC, 2001.
- MATOUŠOVÁ, M., HEJLÍK, L. *Osobní údaje a jejich ochrana.* 2. vyd. Praha: Wolters Kluwer, 2008.
- MATOUŠOVÁ, M. a kol. *Ochrana osobních údajů v otázkách a odpovědích.* 1. vyd. Praha: ASPI Publishing, 2004.

- MORÁVEK, J. *Ochrana osobních údajů v pracovněprávní agendě.* 1. vyd. Praha: BMSS Start, 2010.
- PICHRT, J. *Právo zaměstnanců na nadnárodní informace a projednání.* 1. vyd. Praha: C.H. Beck, 2010.

Periodika

- BARTÍK, V., JANEČKOVÁ, E. Ochrana soukromí na pracovišti – e-mailová pošta. *Práce a mzda.* 2009, č. 11, s. 28-32.
- BARTÍK, V., JANEČKOVÁ, E. Likvidace osobních údajů jako součást zpracování. *Právní rádce.* 2010, č. 2, s. 33-36.
- BARTÍK, V., JANEČKOVÁ, E. Kamery se záznamovým zařízením na pracovišti. *Práce a mzda.* 2010, č. 3, s. 29-33.
- BARTÍK, V., JANEČKOVÁ, E. Poskytování osobních údajů o zaměstnancích. *Práce a mzda.* 2010, č. 10, s. 22-25.
- BARTÍK, V., JANEČKOVÁ, E. Zpracování osobních údajů před uzavřením pracovního poměru. *Personální a sociálně právní kartotéka.* 2010, č. 11, s. 1-6.
- BARTÍK, V., JANEČKOVÁ, E. Jak plnit informační povinnost podle zákona o ochraně osobních údajů. *Právní rádce.* 2011, č. 5, s. 32-35.
- CHLÁDKOVÁ, A. Osobní spis zaměstnance. *Personální a sociálně právní kartotéka.* 2008, č. 6, s. 4-7.
- JANEČKOVÁ, E., BARTÍK, V. Vedení osobního spisu z pohledu ochrany osobních údajů. *Personální a sociálně právní kartotéka.* 2010, č. 7, s. 1-4.
- JOUZA, L. Ochrana osobních práv zaměstnance. *Bulletin advokacie.* 2008, č. 6, s. 34-38.
- KOLMAN, P. Správní sankce na úseku ochrany osobních údajů. *Právní rádce*. 2009, č. 10, s. 39-44.
- MALIŠ, P. Ochrana osobních údajů na pracovišti a povinnosti zaměstnavatelů. *Personální a sociálně právní kartotéka.* 2009, č. 12, s. 1-6.
- MORÁVEK, J. BCR (Binding Corporate Rules). *Právo pro podnikání a zaměstnání.* 2009, č. 9, s. 7-14.

- MORÁVEK, J. Kdy je možné evidovat přístup zaměstnance na internet a otevřít jeho e-mailovou poštu? *Právo pro podnikání a zaměstnání.* 2010, č. 3, s. 3-8.
- MORÁVEK, J. Whistleblowing - zákonná opora. *Právo pro podnikání a zaměstnání.* 2009, č. 12, s. 12-17.
- MORÁVEK, J. Whistleblowing – praktické otázky. *Právo pro podnikání a zaměstnání.* 2009, č. 11, s. 12-20.
- PICHRT, J., MORÁVEK, J. Whistleblowing. *Právo pro podnikání a zaměstnání.* 2009, č. 7-8, s. 19-25.
- RANDLOVÁ, N. VÁŇOVÁ, L. Povinnost zachovávat mlčenlivost v pracovněprávním vztahu a ochrana osobních údajů ostatních zaměstnanců. *Personální a sociálně právní kartotéka.* 2009, č. 10, s. 23-24.

Dokumenty Úřadu pro ochranu osobních údajů

(dostupné z http://www.uoou.cz)

- Informační bulletin ÚOOÚ č. 4/2009
- Informační bulletin ÚOOÚ č. 2/2011
- Stanovisko ÚOOÚ č. 1/2006 – Provozování kamerového systému z hlediska zákona o ochraně osobních údajů
- Stanovisko ÚOOÚ č. 2/2008 – Souhlas se zpracováním osobních údajů
- Stanovisko ÚOOÚ č. 1/2009 – Zpracování osobních údajů na základě smluv uzavíraných se zpracovateli (tzv. řetězení zpracovatelů osobních údajů)
- Stanovisko ÚOOÚ č. 2/2009 – Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště
- Stanovisko ÚOOÚ č. 3/2009 – Biometrická identifikace nebo autentizace zaměstnanců
- Stanovisko ÚOOÚ č. 6/2009 – Ochrana soukromí při zpracování osobních údajů
- Stanovisko ÚOOÚ č. 2/2010 – Předání osobních údajů do jiných států
- ÚOOÚ k problémům z praxe č. 4/2002 – Používání rodného čísla

- ÚOOÚ k problémům z praxe č. 2/2005 Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů
- ÚOOÚ k problémům z praxe č. 2/2010 - Dílčí zpracovatel osobních údajů dle rozhodnutí Komise 2010/87/EU ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES
- ÚOOÚ k problémům z praxe č. 3/2010 – K použití fotografie, obrazového a zvukového záznamu fyzické osoby
- ÚOOÚ k problémům z praxe č. 4/2010 – Zveřejňování osobních údajů na internetu
- Výroční zpráva ÚOOÚ za rok 2008.
- Výroční zpráva ÚOOÚ za rok 2009. ISBN 978-80-210-5130-0.
- Výroční zpráva ÚOOÚ za rok 2010. ISBN 978-80-210-5428-8.

Dokumenty Pracovní skupiny 29

(dostupné z http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs[380])

- Stanovisko WP 29 č. 48 ke zpracování osobních údajů v pracovněprávních vztazích ze dne 13.9.2001 (WP 48)
- Pracovní dokument WP 29 č. 74: Předávání osobních údajů do třetích zemí: Použití článku 26 odst. 2 směrnice EU o ochraně údajů na závazná podniková pravidlo pro případy mezinárodního předávání údajů ze dne 3.6.2003 (WP 74)
- Pracovní dokument WP 29 č. 80 o biometrii ze dne 1.8.2003 (WP 80)
- Pracovní dokument WP 29 č. 107 o spolupráci při vydávání společných stanovisek k přiměřeným zárukám vyplývajícím ze závazných podnikových pravidel ze dne 14.4.2005 (WP 107)
- Pracovní dokument WP 29 č. 108 stanovící modelový seznam pro žádost o souhlas s vydáním závazných podnikových pravidel ze dne 14.4.2005 (WP 108)

- Stanovisko WP 29 č. 1/2006 k problematice užívání právních předpisů EU o ochraně údajů na vnitřní postupy oznamování podezření z protiprávního jednání (whistleblowing) v oblasti účetnictví, vnitřních účetních kontrol, záležitostí auditu, boje proti úplatkářství a trestné činnosti v bankovním a finančním sektoru ze dne 1.2.2006 (WP 117)
- Doporučení WP 29 č. 1/2007 o standardní žádosti o schválení závazných podnikových pravidel pro předávání osobních údajů ze dne 10.1.2007 (WP 133)
- Pracovní dokument skupiny WP 29 č. 153 s tabulkou prvků a zásad závazných podnikových pravidel ze dne 24.6.2008 (WP 153)
- Pracovní dokument WP 29 č. 154 o společném rámci pro strukturu závazných podnikových pravidel ze dne 24.6.2008 (WP 154)
- Pracovní dokument WP 29 č. 155 o často kladených otázkách (FAQs) týkajících se závazných podnikových pravidel (BCR) ze dne 24.6.2008 (WP 155)
- Stanovisko WP 29 č. 13/2011 ke geolokačním službám inteligentních mobilních zařízení ze dne 16.05.2011 (WP 185)

Další dokumenty

- Sdělení Komise Evropskému parlamentu, Radě, ECOSOC a Výboru regionů ze dne 4.11.2010 č. KOM(2010) 609 – Komplexní přístup k ochraně osobních údajů v Evropské unii, dostupné z http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_cs.pdf
- Směrnice ČSN ISO/IEC 17799 (369790): Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací

[380] Názvy dokumentů jsou z anglického originálu přeloženy autorkou; nejedná se o oficiální překlad.

- Důvodová zpráva k zákonu č. 101/2000 Sb. - Sněmovní tisk 374/0 (3. volební období Poslanecké sněmovny 1998 - 2002), dostupná z http://www.psp.cz/sqw/text/tiskt.sqw?O=3&CT=374&CT1=0

Judikatura

- Nález Ústavního soudu sp.zn. Pl. ÚS 4/94 ze dne 12.10.1994
- Nález Ústavního soudu sp.zn. II.ÚS 517/99 ze dne 1.3.2000
- Nález Ústavního soudu sp.zn. II.ÚS 82/07 ze dne 17.1.2008
- Rozsudek Evropského soudu pro lidská práva ve věci Özturk proti Německu ze dne 21.2.1984
- Rozsudek Evropského soudu pro lidská práva ve věci Huvig proti Francii ze dne 24.4.1990
- Rozsudek Evropského soudu pro lidská práva ve věci Niemietz proti Německu ze dne 16.12.1992
- Rozsudek Evropského soudu pro lidská práva ve věci Halford proti Spojenému království ze dne 25.6.1997
- Rozsudek Evropského soudu pro lidská práva ve věci Lauko proti Slovensku ze dne 2.9.1998
- Rozsudek Evropského soudu pro lidská práva ve věci Copland proti Spojenému království ze dne 3.4.2007
- Rozsudek Evropského soudního dvora ve věcí Bodil Lindqvist (C-101/01) ze dne 6.11.2003
- Rozhodnutí Nejvyššího soudu sp.zn. 21 Cdo 1839/2008 ze dne 5.5.2009
- Rozhodnutí Nejvyššího soudu sp.zn. 21 Cdo 2633/2008 ze dne 2.7.2009
- Rozhodnutí Nejvyššího správního soudu sp.zn. 3 As 21/2005 ze dne 10.5.2006
- Rozhodnutí Nejvyššího správního soudu sp.zn. 2 Ans 10/2008 ze dne 16.12.2008
- Rozhodnutí Nejvyššího správního soudu sp.zn. 9 As 34/2008 ze dne 12.2.2009
- Rozhodnutí Nejvyššího správního soudu sp.zn. 1 As 98/2008 ze dne 29.7.2009
- Rozhodnutí Nejvyššího správního soudu sp.zn. 1 As 93/2009 ze dne 16.3.2010

Příloha č. 1

Vzor - Souhlas zaměstnance se zpracováváním osobních údajů

I. Úvod

Společnost Alfa s.r.o. *[následují identifikační údaje společnosti]* se jako zaměstnavatel rozhodla z pozice správce ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů (dále jen „zákon“) zpracovávat osobní údaje svých zaměstnanců v rozsahu širším, než vyžaduje zákon, a to především za účelem zvýšení efektivity řízení podniku a zvýšení konkurenceschopnosti společnosti.

II. Rozsah zpracování osobních údajů

Osobní údaje zaměstnanců společnosti Alfa s.r.o., které budou shromažďovány a dále zpracovávány, zahrnují:

- jméno a příjmení, tituly;
- datum a místo narození, rodné číslo a státní příslušnost;
- bydliště;
- pasová fotografie;
- údaje a doklady o dosaženém vzdělání, předchozí praxi a jazykových znalostech;
- výši a strukturu mzdy; přehled půjček poskytnutých zaměstnanci ze strany společnosti;
- rodinný stav, údaje o rodinných příslušnících (děti, manželé), a to konkrétně jméno a příjmení, datum narození a státní příslušnost;
- *[další osobní údaje dle potřeby zaměstnavatele]*.

III. Účel zpracování

Osobní údaje zaměstnanců společnosti Alfa s.r.o. budou v různých časových rozmezích zpracovávány za účelem vytváření, hodnocení a přizpůsobování personálních a odměňovacích systémů, pro zpracovávání modelů podílové účasti zaměstnanců ve společnosti a pro řízení dalších strategických postupů.

IV. Způsob zpracování

Osobní údaje zaměstnanců společnosti Alfa s.r.o. budou zpracovávány manuálně i automatizovaně. K osobním údajům budou mít přístup pověření pracovníci zaměstnavatel na pozici mzdový účetní, personalista a správce IT.

V. Platnost souhlasu

Poskytnutí osobních údajů společnosti Alfa s.r.o. v rozsahu nad rámec stanovený zákonem je dobrovolné. Informaci o tom, které osobní údaje jsou o konkrétního zaměstnance zpracovávány nad rámec zákona, poskytne obratem na ústní či písemné vyžádání personalista společnosti. Souhlas zaměstnance je udělován na období trvání pracovního poměru, nejdéle však na dobu dvaceti let.

VI. Poučení

Zaměstnanec společnosti Alfa s.r.o. má právo na přístup k osobním údajům a právo na opravu osobních údajů. Zjistí-li nebo domnívá-li se zaměstnanec společnosti Alfa s.r.o., že společnost provádí zpracování jeho osobních údajů, které je v rozporu s ochranou jeho soukromého a osobního života nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může požádat společnost Alfa s.r.o. o vysvětlení či požadovat, aby byl odstraněn takto vzniklý stav. Zejména může žádat blokování, provedení opravy, doplnění nebo likvidaci osobních údajů.

Zaměstnanec má právo obrátit se na Úřad pro ochranu osobních údajů se sídlem v Praze 7, Pplk. Sochora 27, a to zejména v případě, kdy společnost Alfa s.r.o. nevyhoví jeho žádosti o vysvětlení či odstranění stavu vzniklého zpracováním jeho osobních údajů, které je v rozporu s ochranou jeho soukromého a osobního života nebo v rozporu se zákonem.

V případě vzniku nemajetkové újmy v důsledku zpracování osobních údajů může zaměstnanec uplatnit svůj nárok podle obecných předpisů (občanský zákoník).

U d ě l u j i tímto **s o u h l a s** ke zpracování mých osobních údajů v rozsahu a pro účely, které jsou uvedeny v tomto oznámení o zpracování údajů, a to na dobu trvání mého pracovního poměru u společnosti Alfa s.r.o., nejdéle však na dobu dvaceti let.

V _____ dne _____

_____

[jméno, příjmení]

zaměstnanec

Příloha č. 2

Vzor - Poučení zaměstnance o provozování kamerového systému

I. Za účelem nepřetržité ochrany majetku společnosti Alfa s.r.o. *[následují identifikační údaje společnosti]*, a to zejména za účelem odvracení krádeží, poškození či zničení předmětů vyšší hodnoty nacházejících se v IT centru a skladu společnosti, tj. v objektu na adrese *[následuje uvedení přesné adresy včetně případného podlaží]*, je v těchto prostorách nainstalován kamerový systém se záznamovým zařízením.

II. Jakožto zaměstnance společnosti Alfa s.r.o. činného v prostorách, které jsou monitorovány výše uvedeným kamerovým systémem, bychom Vás tímto chtěli informovat o jeho provozování, a rovněž o účelu a způsobu jeho provádění. V případě jakýchkoliv dalších dotazů se můžete obrátit i na svého přímého nadřízeného.

III. Používání kamerového systému se řídí následujícími zásadami:

1) Kamery nejsou primárně určeny ke sledování zaměstnanců a jejich výkonnosti či kontrole jejich chování. Hlavním důvodem instalace kamerového systému je zvýšená ochrana majetku společnosti Alfa s.r.o.

2) Náhodně či namátkově získané informace o možných majetkových deliktech ze strany zaměstnanců společnosti Alfa s.r.o. však budou vyhodnocovány v souladu s účelem kamerového systému a budou dále řešeny v souladu s právními předpisy.

3) Ovládání a přístup k záznamům pořízeným kamerovým systémem je průběžně prováděno pověřenými zaměstnanci společnosti Alfa s.r.o. Pověření zaměstnanci jsou povinni zachovávat mlčenlivost ohledně pořízených záznamů a jsou oprávněni získané informace předávat pouze statutárním orgánům a pověřeným vedoucím zaměstnancům společnosti Alfa s.r.o.

4) Ovládání a přístup k záznamům pořízeným kamerovým systémem ze strany dalších osob s výjimkou pověřených zaměstnanců je vyloučeno.

Stejně tak je zakázáno jakékoliv předání či využití získaných informací kromě případů uvedených v předchozích odstavcích.

5) Záznamy pořízené kamerovým systémem jsou archivovány na centrálním serveru společnosti Alfa s.r.o., který je řádně zabezpečen proti jakémukoliv neoprávněnému přístupu. Archivované záznamy jsou do třech pracovních dnů od jejich pořízení průběžně ze serveru mazány. Delší doba archivace je přípustná pouze tehdy, vyplynulo-li by ze záznamů, že došlo k protiprávnímu zásahu do majetku či práv a chráněných zájmů společnosti Alfa s.r.o.

IV. Současně Vás informujeme, že máte v rozsahu § 12 a 21 zákona č. 101/2000 Sb., o ochraně osobních údajů v platném znění, právo na poskytnutí informací o prováděném zpracování osobních údajů a právo požadovat, aby Vaše osobní údaje nebyly zpracovávány v rozporu se zákonem. Máte rovněž právo obrátit se se svým podnětem na Úřad pro ochranu osobních údajů.

V _____ dne _____

_____

Alfa s.r.o.
zaměstnavatel

Potvrzuji, že jsem byl náležitě **informován/a** o zavedení kamerového systému na mém pracovišti, o zásadách jeho užívání, jakož i o svých právech vyplývajících ze zákona č. 101/2000 Sb., o ochraně osobních údajů.

V _____ dne _____

_____

[jméno, příjmení]
zaměstnanec

Resumé

Ochrana osobních údajů v pracovněprávních vztazích

Práce se zabývá ochranou osobních údajů ve vztahu k zaměstnancům jako subjektům údajů a zaměstnavatelem jako osobou, která tyto údaje zpracovává. V úvodu je rozebrána obecná problematika ochrany osobních údajů včetně stručného přehledu právní úpravy v mezinárodním i národním kontextu. Úvodní část dále zahrnuje zejména výklad zákonných definic a popis jednotlivých práv a povinností v oblasti ochrany osobních údajů.

V následující části se autorka věnuje úpravě nakládání s jednotlivými druhy osobních údajů, k jejichž zpracování dochází v souvislosti se vznikem, trváním či zánikem pracovněprávních vztahů, a také vztahu mezi zákonem č. 101/2000 Sb., o ochraně osobních údajů, a zákoníkem práce, jakož i dalšími souvisejícími právními předpisy. Pozornost je věnována rozsahu osobních údajů, které zaměstnavatel může vyžadovat od uchazečů o pracovní pozici, jakož i otázce nezbytnosti souhlasu zaměstnanců se zpracováním osobních údajů zaměstnavatelem. Tato část práce se dále zabývá také zahrnováním některých informací, jako jsou údaje o zdravotním stavu, odsouzení za trestný čin či fotografie, do kategorie citlivých údajů.

Poslední a nejobsáhlejší kapitola je pak zaměřena na vybrané problematiky, které mohou být v současnosti pro řadu zaměstnavatelů velice aktuální. Autorka se zde zabývá otázkou přípustnosti a podmínkám monitoringu zaměstnanců v různých formách (kamerovými systémy, kontrolou elektronické pošty, sledováním využívání internetu, jakož i monitorování prostřednictvím GPS), problematikou předávání osobních údajů zaměstnanců do zahraničí, a to především v rámci nadnárodních společností, a rovněž systémem tzv. whistleblowingu pocházejícím z USA.

Jako přílohy obsahuje rigorózní práce vzory dvou z nejčastěji používaných dokumentů v oblasti ochrany osobních údajů v pracovněprávních vztazích, a to souhlas zaměstnance se zpracováním osobních údajů a poučení zaměstnance o používání kamerového systému na pracovišti.

Abstract

Personal Data Protection in Labour Law Relationships

The thesis deals with personal data protection in relation to employees as a subject of data and an employer as a person processing such data. At the beginning, general issues of personal data protection are analysed, including a short overview of data protection regulations within both an international and domestic context. The introductory part also includes an explanation of terminology and a description of individual rights and obligations in the field of data protection.

In the following part the author concentrates on the regulation of disposal of particular types of personal data that are processed in relation to creation, duration or termination of labour law relationships, and also on the relationship between the Act No. 101/2000 Coll., on Personal Data Protection, and the Labour Code, as well as other related legislation. Attention is devoted to the extent of personal data that the employer may request from candidates for a vacancy, as well as to the necessity of the employee's consent to the processing of their personal data by the employer. This section also discusses inclusion of certain pieces of information, such as information about a health conditions, criminal convictions or photos, into a sensible data category.

The last and longest chapter focuses on specific questions that may represent topical problems for many modern employers. The author reviews the question of permissibility and conditions of different kinds of employee monitoring (video-surveillance systems, checking of electronic mail, screening of internet use as well as GPS monitoring), the problem of employees' personal data transfer abroad especially within international companies, and also a system of whistleblowing originally from the USA.

In the appendix the thesis contains templates of two frequently used documents in the field of data protection in labour law relationships – an agreement of an employee with personal data processing, and information for an employee about the use of a video-surveillance system in a workplace.

KLÍČOVÁ SLOVA – KEY WORDS

ochrana osobních údajů	personal data protection
pracovněprávní vztahy	labour law relationships
sledování zaměstnanců	monitoring of employees